

U.S. Department of Education Federal Student Aid



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Independent Verification & Validation (IV&V) Handbook

Version 4.0

Final

September 17, 2008

Document Version Control

Version	Date	Description
4.0	09/17/2008	<p>This is the third iteration of the IV&V Handbook, providing detailed standards and procedures for IV&V and IV&V related Security Assessments. This update reflects:</p> <ul style="list-style-type: none"> • Major formatting changes to reflect Federal Student Aid standards for documentation, using the <i>Federal Student Aid Document Template</i> • Standards and procedures to reflect updated Department of Education Security Standards and address new approaches to security risk assessments, security evaluations, and continuous monitoring • A continuous refining of IV&V “best practices” to the Federal Student Aid environment • Updating of Reports and the addition of an Executive Level Report, a Project Funds Tracking Report, and a new Security Roster • Synchronization with the Work Products Guide, updated Production Readiness Review (PRR) Process Guide, and the Enterprise Testing Standards Handbook
3.0	02/15/2006	Final

Table of Contents

Document Version Control	i
Executive Summary	xi
Section 1. Introduction.....	1
1.1 Purpose.....	1
1.1.1 Scope.....	1
1.2 Intended Audience	2
1.3 Document Organization.....	4
1.4 References and Related Documents.....	4
1.5 Introduction to IV&V and Security Assessment	4
1.5.1 Independent Verification & Validation (IV&V).....	4
1.5.2 Security Assessment	5
1.5.3 Federal Student Aid	6
1.5.4 IV&V Requirement and Justification	6
1.5.5 IV&V Process	7
1.5.6 Independence of IV&V.....	8
1.5.7 IV&V Purpose and Goals	8
1.5.8 Assumptions.....	9
1.5.9 Tailoring.....	10
Section 2. Independent Verification & Validation (IV&V) Standards.....	11
2.1 Overview.....	11
2.2 IV&V Organization	11
2.3 IV&V Team Oriented Approach	12
2.3.1 Overview.....	12
2.3.2 Communication.....	12
2.3.3 IV&V Team Qualifications.....	14
2.4 IV&V Guidelines	14
2.4.1 Lifecycle Management Framework (LCM), Enterprise Testing Standards Handbook, and Work Products.....	14
2.4.2 Relevant Federal Guidance	14
2.4.3 Capability Maturity Model Integration (CMMI)	15
2.4.4 Other Standards.....	16
2.5 Key External Organizations.....	16
2.5.1 Virtual Data Center (VDC).....	16
2.5.2 Developer Quality Assurance	17
2.5.3 CIO IT Management	17
2.5.4 Enterprise Operational Change Management (EOCM).....	17
2.5.5 Other Organizations	17
2.6 Standards for IV&V Activities	18
2.6.1 Risk Analysis	20
2.6.2 Verify Entrance/Exit Criteria.....	21
2.6.3 Product Assessment Activities.....	21
2.6.4 Monitor System Development and Test	24

2.6.5	Independent Testing.....	25
2.6.6	Metrics Analysis.....	25
2.6.7	Special Studies.....	25
2.6.8	Periodic Reviews.....	26
2.6.9	Process Assessment Activities.....	26
2.6.10	In Process Reviews.....	27
2.6.11	Anomaly and Proposed Change Evaluation.....	27
2.6.12	Optional IV&V Tasks.....	28
2.7	IV&V Tools.....	30
2.7.1	Computer Aided Software Engineering (CASE) Tools.....	30
2.7.2	Requirements Management Tools.....	30
2.7.3	Configuration Management Tools.....	31
2.7.4	Test Tools.....	31
2.7.5	Model Verification and Analysis Tools.....	31
2.8	IV&V Engagement and Tailoring Strategies.....	31
2.8.1	Lifecycles.....	32
2.8.2	Waterfall.....	32
2.8.3	Prototyping.....	34
2.8.4	Spiral.....	35
2.8.5	Staged Delivery.....	35
2.8.6	Hybrid Approaches.....	36
2.8.7	Commercial Off-The Shelf (COTS) Software.....	36
2.8.8	Rapid Application Development (RAD).....	37
2.8.9	Development Environments.....	37
2.8.10	Externally Imposed Constraints.....	38
2.8.10.1	Budgetary Constraints.....	38
2.8.10.2	Delayed IV&V.....	38
2.8.10.3	EDSS Phased Contract Approach.....	40
Section 3.	Independent Verification & Validation (IV&V) Procedures.....	41
3.1	Overview.....	41
3.2	Management of IV&V.....	41
3.2.1	IV&V Plan Generation.....	41
3.2.2	Baseline Change Assessment.....	42
3.2.3	Management and Technical Review Support.....	42
3.2.4	Interface with Organizational and Supporting Processes.....	42
3.2.5	Federal Student Aid LCM and Work Products Guide.....	42
3.3	LCM Vision Stage.....	45
3.3.1	Vision Stage – Document Reviews.....	45
3.3.2	Vision Stage – Risk Analysis.....	46
3.3.3	Vision Stage – In Process & Stage Gate Reviews.....	47
3.3.4	Vision Stage – Process Reviews.....	48
3.3.5	Vision Stage – Feasibility Analysis.....	49
3.3.6	Vision Stage – High Level System Requirements Evaluation.....	50
3.3.7	Vision Stage – Security Activities.....	50
3.3.8	Vision Stage – IV&V Metrics.....	51
3.4	LCM Definition Stage.....	52

3.4.1	Definition Stage – Document Reviews.....	52
3.4.2	Definition Stage – Requirements and Traceability Analysis.....	53
3.4.3	Definition Stage – Interface Requirements Analysis.....	53
3.4.4	Definition Stage – COTS Products Evaluations.....	54
3.4.5	Definition Stage – In Process & Stage Gate Reviews.....	54
3.4.6	Definition Stage – Process Reviews.....	56
3.4.7	Definition Stage – Risk Analysis.....	56
3.4.8	Definition Stage – Design Evaluation and Traceability Analysis.....	57
3.4.9	Definition Stage – Software Development Folder Reviews.....	58
3.4.10	Definition Stage – Security Activities.....	59
3.4.11	Definition Stage – Section 508 Compliance Review.....	60
3.4.12	Definition Stage – IV&V Metrics.....	61
3.5	LCM Construction and Validation Stage.....	61
3.5.1	Construction and Validation Stage – Document Reviews.....	61
3.5.2	Construction and Validation Stage – Performance Model Evaluation.....	62
3.5.3	Construction and Validation Stage – Peer Reviews.....	63
3.5.4	Construction and Validation Stage – In Process & Stage Gate Reviews.....	63
3.5.5	Construction and Validation Stage – Build Solution Source Code Traceability and Evaluation.....	64
3.5.6	Construction and Validation Stage – Build Solution Unit Code and Logic Walkthroughs.....	65
3.5.7	Construction and Validation Stage – Build Solution Unit Test Analysis.....	66
3.5.8	Construction and Validation Stage – Test Readiness Review Support.....	66
3.5.9	Construction and Validation Stage – Physical Test Environment Review.....	67
3.5.10	Construction and Validation Stage – Test Evaluation.....	68
3.5.11	Construction and Validation Stage – IV&V Test Procedure Development.....	70
3.5.12	Construction and Validation Stage – Test Reporting and Results Analysis.....	71
3.5.13	Construction and Validation Stage – Risk Analysis.....	71
3.5.14	Construction and Validation Stage – IV&V Metrics.....	72
3.5.15	Construction and Validation Stage – Security Activities.....	73
3.5.16	Construction and Validation Stage – Section 508 Checklist Compliance Verification.....	74
3.5.17	Construction and Validation Stage – Readiness Reviews and PRR Support.....	74
3.6	LCM Implementation Stage.....	75
3.6.1	Implementation Stage – Document Reviews.....	76
3.6.2	Implementation Stage – Transition, Production Walkthroughs and Monitoring.....	76
3.6.3	Implementation Stage – Regression Test Monitoring.....	77
3.6.4	Implementation Stage – Installation Configuration Review.....	78
3.6.5	Implementation Stage – Security Activities.....	79
3.6.6	Implementation Stage – Risk Analysis.....	80
3.6.7	Implementation Stage – IV&V Final Report and Lessons Learned Generation.....	80
3.6.8	Implementation Stage – IV&V Metrics.....	81
3.7	LCM Support and Improvement Stage.....	81
3.7.1	Support and Improvement Stage – Document Reviews.....	82
3.7.2	Support and Improvement Stage – Post Implementation Review (PIR) Support.....	82
3.7.3	Support and Improvement Stage – Security Activities.....	83

3.7.4	Support and Improvement Stage – Risk Analysis	83
3.7.5	Support and Improvement Stage – IV&V Metrics	84
3.8	LCM Retirement Stage	84
3.8.1	Retirement Stage – Document Reviews	85
3.8.2	Retirement Stage – Risk Analysis.....	85
3.8.3	Retirement Stage – IV&V Metrics	86
Section 4.	Security Assessment Standards and Procedures	87
4.1	Overview.....	87
4.1.1	Scope.....	88
4.1.2	Assumptions.....	88
4.1.3	Tailoring.....	89
4.2	Application of Security Assessment Standards	89
4.2.1	Laws, Regulations, Standards, and Guidelines.....	89
4.2.2	Security Policy and Procedures	90
4.2.3	Security Assessment Standards.....	92
4.2.4	Future NIST Security and IV&V Related Guidelines	93
4.2.5	Performance-Based Features	95
4.3	Security and the Lifecycle Management Framework (LCM).....	95
4.3.1	Vision Stage.....	96
4.3.2	Definition Stage	97
4.3.3	Construction & Validation Stage	98
4.3.4	Implementation Stage	99
4.3.5	Support and Improvement Stage.....	100
4.3.6	Retirement Stage.....	101
4.4	Security Assessment Methodology.....	101
4.4.1	Approach and Preparation.....	103
4.4.2	Security Assessment Team (SAT) and Resource Requirements	103
4.5	The Risk Assessment Process.....	104
4.5.1	Risk Assessment Methodology.....	104
4.5.2	Evaluating the Risk Assessment Report	109
4.6	The Security Test and Evaluation (ST&E) Process.....	110
4.6.1	Security Test and Evaluation (ST&E) Methodology.....	110
4.6.2	Evaluating the Security Test and Evaluation (ST&E) Report	111
4.7	The Security Certification and Accreditation (C&A) Process.....	112
4.7.1	Overview of Security Certification and Accreditation (C&A).....	112
4.7.2	The Certification Package.....	113
4.7.3	Evaluating the Certification Package.....	113
4.7.3.1	System Security Plan (SSP).....	113
4.7.3.2	System Risk Assessment.....	114
4.7.3.3	Configuration Management Plan (CMP).....	115
4.7.3.4	Continuity of Support/Contingency Plan.....	116
4.7.3.5	Security Test and Evaluation (ST&E)	117
4.7.3.6	Certification Statement/Recommendation	118
4.7.3.7	Accreditation Statement.....	118
4.7.3.8	Corrective Action Plan.....	119
4.8	OVMS Processes and the Performance Improvement Plan Portal	120

4.8.1	Recommendation for Closure Forms (RFC).....	120
4.9	Assessment of Security Design and Architectures	121
4.9.1	General.....	121
4.9.2	Evaluating Technical Architecture Controls.....	121
4.9.2.1	Technical Architecture Controls.....	122
4.9.2.2	Security and Privacy Requirements.....	122
4.9.2.3	System Interfaces.....	122
4.9.2.4	Network Design and Controls.....	122
4.9.2.5	External Interfaces	123
4.9.2.6	Custom and COTS Software.....	123
4.9.2.7	Management/Operational Controls Assessment.....	123
4.9.2.8	Architecture Risk Calculations	124
4.9.2.9	Recommendations.....	124
4.9.3	Evaluating the Four Aspects of Network Defense.....	125
4.9.3.1	Protecting.....	125
4.9.3.2	Detecting.....	125
4.9.3.3	Responding.....	126
4.9.3.4	Sustaining.....	126
4.9.4	Recommendations.....	126
4.9.4.1	Executive Summary	127
4.9.4.2	Introduction.....	127
4.9.4.3	Information Security Analysis	127
4.9.4.4	Findings.....	127
4.9.4.5	Recommendations.....	128
4.9.4.6	Conclusion	128
4.9.4.7	Appendices.....	128
4.10	Vulnerability Scanning and Penetration Testing	128
4.10.1	Approach.....	131
4.10.1.1	Rules of Engagement (ROE) including Letter of Authority (LOA).....	131
4.10.1.2	Setting the Scope of Scanning/Testing (including Third Party Connections and Systems).....	131
4.10.2	Technical Evaluation Activities.....	132
4.10.2.1	Port Scanning.....	132
4.10.2.2	SNMP Scanning.....	132
4.10.2.3	Enumeration & Banner Grabbing.....	132
4.10.2.4	Wireless Enumeration.....	132
4.10.2.5	Vulnerability Scanning.....	132
4.10.2.6	Host Evaluation.....	132
4.10.2.7	Network Device Analysis	133
4.10.2.8	Password Compliance Testing.....	133
4.10.2.9	Application Specific Scanning.....	133
4.10.2.10	Network Sniffing	133
4.10.2.11	War Dialing.....	133
4.10.2.12	Denial of Service.....	133
4.10.2.13	Penetration Testing	133
4.10.3	Evaluating Vulnerability Scanning and Penetration Testing Results	134

4.10.3.1	Introduction.....	134
4.10.3.2	Scope.....	134
4.10.3.3	Assumptions.....	134
4.10.3.4	Tailoring.....	134
Section 5. Independent Verification & Validation (IV&V) Reporting Standards and Procedures		
	136	
5.1	Overview.....	136
5.1.1	Documentation Control.....	136
5.1.2	Walkthroughs for Federal Student Aid Deliverables.....	137
5.1.2.1	Planning the Walkthrough	138
5.1.2.2	Preparing the Meeting Notice	138
5.1.2.3	Distributing Review Materials	138
5.1.2.4	Reviewing the Materials	139
5.1.2.5	Performing the Walkthrough	139
5.1.2.6	Resolving Defects/Issues	140
5.1.2.7	Verifying Defect/Issue Resolution.....	140
5.1.2.8	Completing the Walkthrough.....	140
5.1.2.9	Filing the Walkthrough Materials.....	140
5.2	IV&V Reporting Standards and Procedures.....	140
5.2.1	Reporting Overview.....	141
5.2.2	Reporting Templates.....	141
5.2.2.1	IV&V Plan	141
5.2.2.2	Review Plan	143
5.2.2.3	Completed Checklists	144
5.2.2.4	Technical Reports	144
5.2.2.5	Document Review Comments	145
5.2.2.6	Memorandum of Record (MOR).....	146
5.2.2.7	Review Report	146
5.2.2.8	Feasibility Assessment Report.....	146
5.2.2.9	Requirements Verification Matrix (RVM).....	147
5.2.2.10	Anomaly Report.....	147
5.2.2.11	Risk Assessment Report and Risk Watch List.....	147
5.2.2.12	IV&V Test Procedures and Use Cases	148
5.2.2.13	Test Report.....	148
5.2.2.14	Special Studies Report	149
5.2.2.15	IV&V End of Phase Summary Report.....	149
5.2.2.16	Production Readiness Review Recommendation	150
5.2.2.17	IV&V Final Report	151
5.2.2.18	Progress Report.....	151
5.2.2.19	Trip Report.....	152
5.2.2.20	IV&V Metrics Report	152
5.2.2.21	Funds Expended Report.....	153
5.2.2.22	Contractor Team/Security Roster	153
5.2.2.23	Executive Level Project Report	153
5.2.2.24	IV&V Lessons Learned	154
5.3	Security Reporting Standards and Procedures.....	154

Section 6. Independent Verification & Validation (IV&V) Performance Standards and Procedures 155

6.1	Overview.....	155
6.1.1	Objectives	155
6.1.2	Performance Assessment	156
6.2	IV&V Performance Standards and Procedures.....	157
6.2.1	Performance Assessment Areas.....	158
6.2.2	Performance Assessment Ratings.....	160
6.3	IV&V Metrics	161
6.3.1	Methodology.....	161
6.3.2	Reporting.....	162
6.3.2.1	IV&V Metrics Report Outline	164
6.3.2.2	Metrics Scoring Example.....	164
6.3.2.3	Enterprise Quality Assurance IV&V Metrics Tracking and Reporting.....	165
Appendix A: Acronyms and Abbreviations.....		A-2
Appendix B: Glossary.....		B-2
Appendix C: IV&V Checklists		C-2
Appendix D: Risk Management Process		D-2
Appendix E: IV&V Reporting Templates		E-2
Appendix F: Security Assessment Questionnaire.....		F-2
Appendix G: Miscellaneous Security Templates.....		G-2
Appendix H: Performance Assessment Sample Questions and Survey		H-2
Appendix I: IV&V Metrics Dashboard.....		I-2
Appendix J: Bibliography and References		J-2

List of Exhibits

Exhibit 2- 1, IV&V Iterative Feedback Process	13
Exhibit 2- 2, Mandatory IV&V Tasks	18
Exhibit 2- 3, Optional IV&V Tasks.....	19
Exhibit 2- 4, Comparison of Full IV&V to RAD IV&V and Externally Constrained IV&V	39
Exhibit 3- 1, Federal Student Aid IV&V Lifecycle Activities	44
Exhibit 4- 1, Security Assessment Activities During the LCM Stages	96
Exhibit 4- 2, Security Architecture Risk Calculations.....	124
Exhibit 5- 1, IV&V Reporting Requirements	141
Exhibit 5- 2, Review Plan	143
Exhibit 5- 3, Review Report	146

List of Figures

Figure 4- 1, ST&E Methodology	111
-------------------------------------	-----

List of Tables

Table 1- 1, Intended Audience and Document Uses.....	2
Table 2- 1, Waterfall	32
Table 2- 2, Overlapping Waterfall	33
Table 2- 3, Waterfall with Subprojects	34
Table 2- 4, Waterfall with Risk Reduction	34
Table 2- 5, Prototyping	35
Table 2- 6, Spiral.....	35
Table 2- 7, Staged Delivery	36
Table 2- 8, COTS Software	36
Table 3- 1, Vision Stage - Document Reviews.....	45
Table 3- 2, Vision Stage - Risk Analysis.....	47
Table 3- 3, Vision Stage - In Process & Stage Gate Reviews	48
Table 3- 4, Vision Stage - Process Reviews	48
Table 3- 5, Vision Stage - Feasibility Analysis	49
Table 3- 6, Vision Stage - High Level System Requirements Evaluation.....	50
Table 3- 7, Vision Stage - Security Activities	51
Table 3- 8, Vision Stage - IV&V Metrics.....	51
Table 3- 9, Definition Stage - Document Reviews	52
Table 3- 10, Definition Stage - Requirements and Traceability Analysis	53
Table 3- 11, Definition Stage - Interface Requirements Analysis	54
Table 3- 12, Definition Stage - COTS Products Evaluations	54
Table 3- 13, Definition Stage - In Process & Stage Gate Reviews.....	55
Table 3- 14, Definition Stage - Process Reviews	56
Table 3- 15, Definition Stage - Risk Analysis	56
Table 3- 16, Definition Stage - Design Evaluation and Traceability Analysis.....	57
Table 3- 17, Definition Stage - Software Development Folder Reviews	59
Table 3- 18, Definition Stage - Security Activities.....	60
Table 3- 19, Definition Stage - Section 508 Compliance Review	60
Table 3- 20, Definition Stage - IV&V Metrics	61
Table 3- 21, Construction and Validation Stage - Document Reviews	62
Table 3- 22, Construction and Validation Stage - Performance Model Evaluation	62
Table 3- 23, Construction and Validation Stage - Peer Reviews.....	63
Table 3- 24, Construction and Validation Stage - In Process & Stage Gate Reviews.....	63
Table 3- 25, Construction and Validation Stage - Build Solution Source Code Traceability and Evaluation	64
Table 3- 26, Construction and Validation Stage - Build Solution Unit Code and Logic Walkthroughs.....	65
Table 3- 27, Construction and Validation Stage - Build Solution Unit Test Analysis	66
Table 3- 28, Construction and Validation Stage - Test Readiness Review Support.....	67
Table 3- 29, Construction and Validation Stage - Physical Test Environment Review	68

Table 3- 30, Construction and Validation Stage - Test Evaluation	68
Table 3- 31, Construction and Validation Stage - IV&V Test Procedure Development.....	70
Table 3- 32, Construction and Validation Stage - Test Reporting and Results Analysis	71
Table 3- 33, Construction and Validation Stage - Risk Analysis	72
Table 3- 34, Construction and Validation Stage - IV&V Metrics	72
Table 3- 35, Construction and Validation Stage - Security Activities.....	73
Table 3- 36, Construction and Validation Stage - Section 508 Checklist Compliance Verification	74
Table 3- 37, Construction and Validation Stage - Readiness Reviews and PRR Support.....	75
Table 3- 38, Implementation Stage - Document Reviews	76
Table 3- 39, Implementation Stage - Transition, Production Walkthroughs and Monitoring.....	77
Table 3- 40, Implementation Stage - Regression Test Monitoring.....	78
Table 3- 41, Implementation Stage - Installation Configuration Review	79
Table 3- 42, Implementation Stage - Security Activities.....	79
Table 3- 43, Implementation Stage - Risk Analysis	80
Table 3- 44, Implementation Stage - IV&V Final Report and Lessons Learned Generation.....	80
Table 3- 45, Implementation Stage - IV&V Metrics	81
Table 3- 46, Support and Improvement Stage - Document Reviews	82
Table 3- 47, Support and Improvement Stage - Post Implementation Review (PIR) Support.....	82
Table 3- 48, Support and Improvement Stage - Security Activities	83
Table 3- 49, Support and Improvement Stage - Risk Analysis.....	84
Table 3- 50, Support and Improvement Stage - IV&V Metrics	84
Table 3- 51, Retirement Stage - Document Reviews.....	85
Table 3- 52, Retirement Stage - Risk Analysis.....	85
Table 3- 53, Retirement Stage - IV&V Metrics.....	86
Table 4- 1, SDLC Stages and Related Risk Assessment Activities.....	105
Table 4- 2, Required Level of Effort for Risk Assessment.....	115
Table 4- 3, ST&E Levels of Effort by Certification Tier	117
Table 4- 4, OVMS 8 Step Process	120
Table 6- 1, IV&V Metrics Categories.....	162

Executive Summary

Federal Student Aid manages an ambitious portfolio of information systems to provide services to its customers: students, parents, borrowers, and trading partners (institutions of higher education, lenders, and guaranty agencies). Due to the high visibility and national impact of Title IV Student Financial Assistance Programs, IV&V is one of the tools that Federal Student Aid utilizes during software application development and enhancement projects. As a Performance Based Organization, Federal Student Aid desires to establish standards and criteria to measure the performance of its IV&V agents.

The IV&V approach presented in this handbook facilitates a team-building relationship between the developers and IV&V staff. The approach features open lines of communication and cooperation between the two groups while maintaining independence and objectivity of and by the IV&V staff. This approach is enhanced through risk based monitoring of the targeted processes and products in a structured manner and features timely communication of findings to the development organization.

This handbook is structured to include standards and procedures for:

- Conducting IV&V Reviews
- Security Effectiveness Evaluations
- IV&V Reporting
- IV&V Performance Measures

Each of these standards and procedures has been combined into this Handbook. The purpose of this handbook is to establish standards and procedures for conducting IV&V and assessing the information security of designated Federal Student Aid systems under development and in production.

Section 1. Introduction

1.1 Purpose

This IV&V Handbook was developed to establish standards and procedures for conducting IV&V reviews and system security assessments of information technology systems supporting Federal Student Aid, U.S. Department of Education. This handbook defines Federal Student Aid's expectations for contractors performing IV&V and the procedures to be followed. Any tailoring of these standards and procedures should be approved by the Enterprise Quality Assurance Team.

These standards and procedures were developed and tailored using relevant portions of the Institute of Electrical and Electronics Engineers (IEEE) Standard (STD) 1012-1988 "Standard for Software Verification and Validation" as a guide for IV&V and various National Institute of Standards and Technology (NIST) Publications, as outlined in Section 4.

Execution of IV&V and system security assessment and reviews that follow the accompanying guidelines will help to insure that IV&V and security assessment teams can consistently meet the quality and performance requirements of Federal Student Aid in an effective, timely and cost effective manner. In addition, adherence to these IV&V and security assessment guidelines will accomplish these specific objectives:

- Provide objective system development and system security risk assessment appraisals
- Adherence to Federal guidance governing management and review of systems development and security assessment activities
- Increased Federal Student Aid visibility into development activities
- Increased requirements and design phase visibility
- Early problem identification and remediation strategy development
- Reduce risk associated with systems development
- Reduce security threats and vulnerabilities to systems throughout the Lifecycle Management Framework (LCM)
- Improved system maintainability, reliability and integrity

1.1.1 Scope

This IV&V Handbook describes the activities to be conducted for Federal Student Aid system acquisition and development. The IV&V Team will perform IV&V activities for each target system, as directed by Federal Student Aid.

These standards and procedures are appropriate for application to software acquired or developed by Federal Student Aid. These IV&V standards and procedures will describe the following:

- Verification of program development products and processes and evaluation of each product against all previous development phase product requirements

- Validation that the completed end product complies with established software and system requirements
- Guidance for tailoring IV&V activities based on lifecycle methodology, development environment, and externally imposed constraints

For each target system to undergo IV&V, it is recommended that a project-specific IV&V Plan be prepared that briefly specifies the target system profile, organization of the IV&V Team, scope of the IV&V effort, points of contact for all parties, and tailoring of any IV&V tasks or checklists. Federal Information Processing Standards (FIPS) Publication 132, “Guideline for Software Verification and Validation Plans” provides a guide for developing IV&V Plans.

1.2 Intended Audience

The table below lists the intended users for the IV&V Handbook, the document sections most relevant for each type of user, and the purpose for which the users may utilize the information in this document.

Table 1- 1, Intended Audience and Document Uses

Intended Audience and Document Uses		
Users	Relevant Sections	Uses
Enterprise Quality Assurance IV&V	Section 1 Introduction	Provides a general introduction to the structure of the IV&V Handbook including its purpose and goals. This section also provides IV&V analysts with an understanding and definition of the importance of independence.
Enterprise Quality Assurance IV&V	Section 2 Independent Verification & Validation (IV&V) Standards	IV&V Standards, to include the resources, tools, techniques, and methodologies necessary to perform software verification and validation of the target systems.
Enterprise Quality Assurance IV&V	Section 3 Independent Verification & Validation (IV&V) Procedures	Standards and procedures for the IV&V tasks to be performed throughout the stages of the Lifecycle Management Framework (LCM).
Enterprise Quality Assurance Federal Student Aid Security Personnel	Section 4 Security Assessment Standards and Procedures	Standards and procedures for evaluating the compliance of Federal Student Aid systems with Federal Information Security policies and to perform evaluations of the security effectiveness of Federal Student Aid information systems security controls.

Intended Audience and Document Uses		
Users	Relevant Sections	Uses
Enterprise Quality Assurance IV&V Team	Section 5 Independent Verification & Validation (IV&V) Reporting Standards and Procedures	Reporting requirements necessary for the IV&V Team to fully document its activities for Federal Student Aid target systems throughout their development and implementation.
Enterprise Quality Assurance IV&V Team	Section 6 Independent Verification & Validation (IV&V) Performance Standards and Procedures	Performance measurement system and associated requirements necessary for the IV&V Team to document its activities in a measurable format for Federal Student Aid.
Federal Student Aid Security Personnel Enterprise Quality Assurance IV&V Team	Appendix C IV&V Checklist	Fundamental tools maintained by the IV&V Team for use during evaluations.
Enterprise Quality Assurance IV&V Team	Appendix D Risk Management Process	Project management tool used to codify good management techniques meant to identify and control the risks inherent in any software development process.
Enterprise Quality Assurance IV&V Team	Appendix E IV&V Reporting Templates	This section provides the templates required for IV&V task reporting.
Federal Student Aid Security Personnel Enterprise Quality Assurance IV&V Team	Appendix F Security Assessment Questionnaire	This section provides a reference for types of questions required for Security Assessments.
Federal Student Aid Security Personnel	Appendix G Miscellaneous Security Templates	Provides sample templates for execution of security reviews and reporting.
Enterprise Quality Assurance IV&V Team	Appendix H Performance Assessment Sample Questions and Survey	This template provides a template for the Federal Student Aid contractor survey completed by Federal Student Aid staff to assess the quality and effectiveness of the work performed.
Enterprise Quality Assurance IV&V Team	Appendix I IV&V Metrics Dashboard	Provides a template for reporting IV&V Metrics to Federal Student Aid Management.

1.3 Document Organization

This document comprises the following sections.

Section 1 – Introduction: is an Introduction to IV&V and Security Assessment.

Section 2 - Independent Verification and Validation Standards: covers Independent Verification and Validation Standards.

Section 3 - Independent Verification and Validation Procedures: covers Independent Verification and Validation Procedures.

Section 4 - Security Assessment Standards and Procedures: covers Security Assessment Standards and Procedures.

Section 5 - Independent Verification and Validation Reporting Standards and Procedures: covers Reporting Standards and Procedures for both IV&V and Security Assessment.

Section 6 - Independent Verification and Validation Performance Standards and Procedures: covers Performance Standards and Procedures for both IV&V and Security Assessment including IV&V Metrics.

Appendix A - Acronyms and Abbreviations

Appendix B - Glossary

Appendix C - IV&V Checklists

Appendix D - Risk Management Process

Appendix E - IV&V Report Templates

Appendix F - Security Assessment Questionnaire

Appendix G - Miscellaneous Security Templates

Appendix H - Performance Assessment Sample Questionnaire and Survey

Appendix I - IV&V Metrics Dashboard

Appendix J - Bibliography and References

1.4 References and Related Documents

For information on the guidance and references that were used to create this document, see Appendix J.

1.5 Introduction to IV&V and Security Assessment

1.5.1 Independent Verification & Validation (IV&V)

IV&V is a process, independent of the development organization, used to assure that the products of a system development activity meet the requirements of that activity and that the delivered system satisfies the intended use and user needs as described to the developer.

Verification ensures that standard procedures and practices as defined in the Federal Student Aid LCM Framework are followed. Requirements are verified and development products are evaluated against defined requirements. Deliverables are examined to ensure that they are standardized as applicable under the LCM, are accurate, and are delivered in a timely fashion.

Validation ensures that all requirements are adequately tested or demonstrated, and that test results are as expected and can be repeated to verify correct implementation of Federal Student Aid approved changes that are required based on results of testing.

Execution of a plan that follows these guidelines will help to ensure that the IV&V Team can consistently meet the day-to-day quality and performance requirements of Federal Student Aid in a timely and cost-effective manner. Performance of these IV&V activities yields the following:

- An objective system development appraisal
- A baselined set of testable requirements that match the user's needs
- Opportunity to identify problems early in the lifecycle
- Increased requirements and design visibility and traceability
- Early potential problem area indication
- Development risk reduction
- Improved maintainability and reliability

1.5.2 Security Assessment

Traditionally, security assessment is an integral element of a comprehensive IV&V assessment and follows the analytical processes for reviewing system functionality and artifacts described in Sections 1, 2 and 3.

Section 4 of this IV&V Handbook describes standards and procedures for conducting additional types of system security effectiveness evaluations that are beyond the scope of IV&V support efforts. Included are standards and procedures for conducting system security assessments to evaluate whether appropriate security safeguards are implemented and operating effectively throughout the complete LCM.

Security effectiveness evaluations can generally be classified as either:

- Process and artifact reviews
- Risk Assessments
- Continuous Monitoring
- Detailed technical analysis of the system architecture
- Effectiveness of all or specific security management, operational, and technical controls
- Environmental Testing using exploratory techniques directed at probing the vulnerability of the network and/or human components.

Individual subsections describe the standards and procedures for conducting the following types of security evaluations on Federal Student Aid information systems:

- Application of Security Assessment Standards
- LCM Security Activities
- Security Assessment Methodology
- Risk Assessment Methodology
- Security Test and Evaluations
- Security Certification and Accreditation Process
- Security Corrective Action Process
- Assessment of Security Designs and Architectures
- Vulnerability Scanning and Penetration Testing

1.5.3 Federal Student Aid

The Federal Student Aid organization is designed to ensure effective lines of authority, supervision, and communication in all aspects of systems development, enhancement, and operations work. These standards and procedures describe the authority and specific responsibilities for IV&V teams throughout a target system lifecycle and identify the specific resources necessary to perform IV&V and security assessment tasks effectively.

The Chief Information Officer (CIO) has overall responsibility for instituting and leading the IV&V approach for Federal Student Aid. The Enterprise Quality Assurance Team has the responsibility and authority to provide guidance in the areas of standard practices, procedures, and guidelines in IV&V efforts. In addition, the Enterprise Quality Assurance Team monitors all IV&V tasks to ensure that IV&V contractors meet Federal Student Aid's needs.

Federal Student Aid's Independent Verification & Validation activities utilize a modified form of the technique commonly known as "Integrated Independent Verification & Validation." The IV&V Support contractor is integrated with Federal Student Aid Management in support of the project. Document reviews are expected frequently, often with short turn-around times. This integrated approach ensures that timely feedback is given from Federal Student Aid to the developer to improve program success. The integrated approach to IV&V requires the IV&V contractor to play a much more active role than the traditional role of IV&V.

1.5.4 IV&V Requirement and Justification

The Clinger-Cohen Act of 1996 was passed in response to federal audits that consistently found that waste, fraud, abuse, and mismanagement of information technology (IT) resources were often the result of an inadequate investment process, investment decisions based on unreliable data, and a failure to understand that IT investments must show actual returns in order to pay dividends. In addition, the act was an attempt to reduce an excessive documentation approval process and an overlong acquisition cycle. The legislation is based on proven best practices that are used in the IT industry to improve performance and meet strategic goals. This, in turn, should ensure project completion within schedule, at acceptable costs, and with positive Return On Investment (ROI).

A major provision of the Clinger-Cohen Act calls for performance and results-based management in order to increase the focus on process improvement among other strategic improvements. One of the recommended techniques for this, as described in the “Project Management Handbook for Mission Critical Systems: A Handbook for Government Executives,” is “to outsource for IV&V support.” The Handbook goes on to state “it is critical for the executive leadership to listen to IV&V advice.”

It is difficult to assign dollar numbers and cost effectiveness to IV&V for software development in terms of doing traditional ROI calculations because the process does not lend itself to these measures and very few organizations have built a database of historical metrics that allow for comparisons between similar projects. The kinds of questions that have to be answered in building such a database would include:

- Would the developer have found the same problems?
- If so, when would they have been found and what would have been the cost of correction?
- What would the costs have been in terms of customer impact if the defects had not been detected?

Attempts to answer these questions have been made in case studies comparing similar projects. One involved IV&V throughout the entire lifecycle, and the other was a project that used IV&V in a partial lifecycle (meaning one or more pre-code and development phases were not supported by IV&V). This study determined that the project fully supported by IV&V resulted in a reduction in defects of almost two-thirds compared to the project that was partially supported.

Other important benefits of IV&V include:

- The “watchdog effect” that is recognized as encouraging the developer to be more conscientious and more likely to exercise greater care
- Improved maintainability because of the increased accuracy, readability, and maintainability of system documentation
- Better understanding of and response to risks

These benefits, although not quantifiable, may actually outweigh the benefits of the calculated ROI.

1.5.5 IV&V Process

The IV&V process is part of the systems engineering function and provides objective data and recommendations concerning software quality, software performance, and schedule compliance to Federal Student Aid. The IV&V process can include analysis, evaluation, review, inspection, assessment, and testing of software products and processes within the context of the system.

IV&V is an extension of the program management and systems development team and is best accomplished using a team-building approach since there is a natural conflict for the IV&V Team between maintaining objectivity through organizational independence and remaining a constructive part of the team effort in building quality into the software and the development process. The team-building approach to IV&V is described in greater detail in Section 2.

1.5.6 Independence of IV&V

IV&V independence is established through four mechanisms: technical independence, managerial independence, financial independence, and contractual independence.

- Technical independence requires that IV&V personnel not be involved in any stage of the software development process.
- Managerial independence requires that IV&V responsibility be vested in an organization that is separate from the development and program management organizations. The independent selection of the artifacts to be examined and tested, the techniques to be used, the issues to be chosen, and the reporting to be made further affirm this independence.
- Financial independence requires that the IV&V budget be vested in an organization independent from the development organization.
- Contractual independence requires that the IV&V contract be executed separately from the contract for development.

Traditional IV&V independence is achieved when all four parameters exist by vesting the IV&V authority in an organization separate from the development organization. This requires that the IV&V organization establish a close working relationship with the development organization while maintaining an independent role.

1.5.7 IV&V Purpose and Goals

The IV&V Program objective is to provide an independent system assessment by analyzing and testing the target system to assure that it performs its intended functions correctly, to ensure that it performs no unintended functions, and to measure its quality and reliability. These standards and procedures describe the overall concept and management approach for IV&V and define the responsibilities required to conduct an effective IV&V program.

The intent of verification and validation is to improve the quality of the software during the lifecycle process, not afterwards, and it must be performed at the same time as the software development. It should be done in a manner that provides early feedback to the development organization, allowing modifications to processes and products in a timely fashion. This proactive, but independent, approach -- as compared to an auditing or adversarial approach -- results in fewer delays, reduced cost, higher product quality, and improvement of the development process itself.

The focus of the IV&V standards and procedures is on successful execution of IV&V activities required to ensure the procurement, integration and implementation of high quality new software and upgrades for Federal Student Aid target systems. IV&V activities strive to ensure that quality is built into the system and that it satisfies user requirements. IV&V provides insights into the status of the development activity, allowing for timely correction of identified defects in the products or in the development processes. IV&V employs review, analysis and testing techniques to determine whether a system complies with requirements. These requirements include both functional and performance capabilities defined in the system specifications as well as quality attributes. Quality attributes are identified as those which serve the user's need for a product that is capable of meeting its objectives. Additionally, the IV&V activities endeavor to

ensure that products provided by the developer will provide Federal Student Aid with the software and associated documentation necessary to facilitate future enhancements. Key elements that serve as a foundation for effective IV&V include:

- Domain knowledge
- Rigorous implementation of well-defined analysis processes and procedures
- Structured and thorough assessments
- Correct identification of critical system functions to enable focusing on areas that benefit the most from IV&V, especially critical for rapid application development
- Clear and timely communication of IV&V results
- Effective management of performance objectives
- Senior staff with industry certifications in the appropriate subject matter

Corrections of deficiencies identified during the verification process are evaluated to the lowest applicable level to ensure the integrity of the requirements, design, code, and test evolution. The validation process ensures that all requirements are adequately tested or demonstrated, and that test results are as expected and can be repeated to verify correct implementation of Federal Student Aid approved changes that are required based on results of testing. Performing IV&V as defined in these standards and procedures provides for a comprehensive evaluation throughout each phase of the target system to help ensure that:

- Errors are detected and corrected as early as possible in the software lifecycle
- Project risk, cost, and schedule effects are lessened
- Software quality and reliability are enhanced
- Management visibility into the software process is improved
- Proposed changes and their consequences can be quickly assessed

1.5.8 Assumptions

It is assumed that the IV&V Team has continuous access to developer documentation, status information, configuration management (CM) data, test results, and defects data. The IV&V Team requires early, complete and continuous visibility into the development effort. The IV&V Team must be exposed to all aspects, both formal and informal, of the development effort in order to perform an adequate and accurate assessment. Often, informal processes constitute the essence of a development effort, and observation and participation in these activities by the IV&V Team is beneficial to both parties. The IV&V Team gains technical insight and can capture information that may not be formally documented, and the development team can often benefit from the input of additional qualified technical personnel. The IV&V Team also provides a unique perspective that is not only more objective but also focused on the end goals of the development.

These IV&V standards and procedures are designed to augment the development effort while minimizing interference. In order to implement these standards and procedures, the IV&V Team assumes that, for automated IV&V activities, the required developer's electronic media

documentation, as well as requirements traceability, code analysis, and design evaluation automated tools are available.

1.5.9 Tailoring

These IV&V standards and procedures are a “guide” and will be tailored as appropriate for each target system development in an IV&V Plan. Tailoring of these standards and procedures is to be done by the IV&V Team in consultation with each respective Federal Student Aid organization. The tailoring effort shall include definition of the acceptable level of risk and identification of those software components that are considered critical. The IV&V tasks and procedures may be tailored depending upon the type of system being developed (i.e., new or already deployed), the software development methodology, or the actual software being implemented by the developer (e.g., new code versus reused code). Other factors to consider are the use of an accelerated development, commercial off-the-shelf (COTS)-based development, or custom development.

Section 2. Independent Verification & Validation (IV&V) Standards

2.1 Overview

The following section describes the IV&V standards, to include the resources, tools, techniques, and methodologies necessary to perform software verification and validation of the target systems. These standards apply to all stages of the LCM as described in the LCM Directive from the Vision Stage to the Retirement Stage. These standards necessitate the use of mandatory IV&V tasks, while allowing the IV&V Team to tailor their efforts by selecting any of the optional IV&V tasks, or identifying new tasks to be performed on the target systems.

2.2 IV&V Organization

To ensure an effective IV&V program and timely performance of the prescribed IV&V tasks, the IV&V Team must establish and implement an effective management and control structure. The Federal Student Aid Enterprise Quality Assurance Program Manager will coordinate all IV&V activities, and all formal communications from the Enterprise Quality Assurance Team will be directed through the IV&V Program Manager to the IV&V staff. The IV&V Team's Program Manager will assign tasks and apply the resources necessary to perform these tasks.

The IV&V Team will thoroughly document all IV&V efforts and inform the Federal Student Aid Enterprise Quality Assurance Team of their findings as the tasks are performed. Formal evaluations, comments, process review reports, and technical reports related to IV&V activities will be generated by the IV&V Team and communicated to the developer through the Federal Student Aid Enterprise Quality Assurance Team or the Federal Student Aid development representative. All deliverables will be prepared and submitted to the Federal Student Aid Enterprise Quality Assurance Team. The IV&V Team will utilize checklists to monitor task performance and product delivery. Examples of the checklists that may be used are included in Appendix C.

At each IV&V phase/iteration, planned IV&V activities will be reviewed and new tasks added as necessary, to focus on any critical issues that arise. The IV&V Program Manager will closely monitor the accuracy and quality of all deliverables and IV&V results, as the development staff must allocate resources to address IV&V findings. By ensuring their accuracy and conciseness, the IV&V Program Manager will minimize the impact on the developer's time and resources.

The IV&V Team will be responsible for the following activities:

- Supporting the validation of specified requirements and configuration items
- Providing technical analysis of the development effort, including metrics analysis
- Performing risk analysis during the development lifecycle
- Assisting with the verification of designated data items and products
- Performing requirements and test case traceability analyses

- Monitoring the developer's testing activities
- Preparing and implementing independent test scenarios
- Performing reviews of configuration items and processes
- Providing Integrated Product Team support

The above activities will be performed in accordance with the methodology prescribed in these standards and procedures at the direction of the IV&V Program Manager. Most IV&V tasks, with the exception of testing services, on site reviews, and formal process reviews will be performed at the IV&V Team's offices. The IV&V Team will provide the required resources for the specific IV&V activities detailed in Section 3. The IV&V Team will interface with members of each target system team, as appropriate.

2.3 IV&V Team Oriented Approach

As mentioned in Section 1, there is a natural conflict between the independence of the IV&V Team and the promotion of a team-oriented rather than adversarial relationship with the developer. Both the IV&V Team and the development team must accept as the common driving principle that the objective is to produce the highest quality software possible. While both teams can be expected to have different perspectives and incentives, these views can be constructively used to improve both the processes and the products. Both teams must remain flexible, stay in close communication, and establish an atmosphere of mutual respect. In addition, the IV&V Team will work closely with the developer's internal Quality Assurance and attempt to leverage their activities through information sharing. However, it is critical that IV&V maintain their independence and a clear separation from these two groups.

2.3.1 Overview

The IV&V task of software quality improvement in a team-building environment is accomplished by monitoring the targeted processes in a structured manner. This approach uses proven standards and techniques for objectively identifying data and drawing concrete conclusions related to software quality, performance, and work schedule compliance. These findings are then communicated to the development organization and client through the use of timely and constructive feedback.

2.3.2 Communication

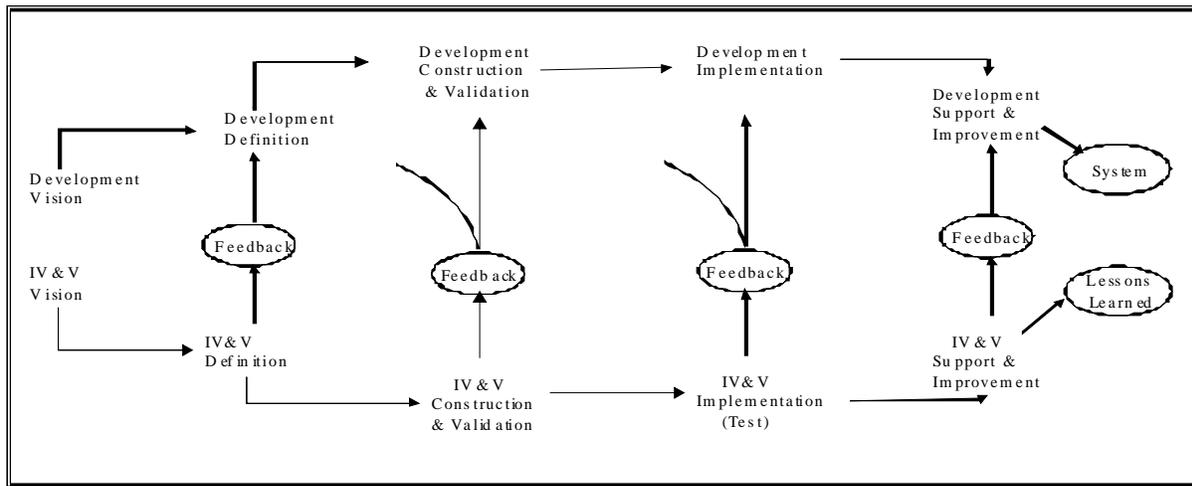
Team-building in this environment depends on "heads up" communication as opposed to an auditing approach that is intended to identify deficiencies and that may, inevitably, provide late feedback. This "heads up" approach is accomplished by means of feedback that is timely, relevant, constructive, and aimed at improving the development process during the lifecycle. The objective is to build trust, not destroy it. There are several means of providing constructive feedback to the development team and the client organization. These may include, but are not limited to, e-mail alerts, status reports, issue logs, a risk watch list, and formal and informal reviews and findings. Informal verbal comments and briefings on minor process items, such as suggestions for additional methods or improvements, may be appropriate but should be documented for the IV&V customer. This communication approach lays the groundwork for

building rapport between the developers and the IV&V team. The communication methods employed are largely determined by the development methodology being used and the degree of impact of the findings involved.

It is vitally important that these findings and recommendations be provided to the development organization in a manner and format that allows the developer to rapidly integrate them into the development process. They should be prioritized in terms of impact, relevance, and audience so that the appropriate member of the development team can focus on the most important issues first. Minor issues, such as recurring typos or minor documentation errors, should be summarized rather than presented as a series of issues, so they do not obscure the more important findings. This feedback process is iterative and spans the development lifecycle but does not substitute for entrance and exit criteria at predetermined points in the lifecycle. Exhibit 2-1 shows the parallel tracks of development and IV&V activities through the first four stages of the LCM. Arrows indicate the IV&V feedback that applies to the parallel development stage and previous development stages.

In those rare instances where this approach to process improvement is not possible, it may be necessary to adopt a more traditional approach to IV&V that focuses on documenting deficiencies. It should be noted that if this is deemed necessary, this may be a warning sign of there being potentially serious problems with the development project, and the customer should be notified of this. It must always be kept in mind that the primary IV&V objective is to protect the client’s interests in the development project by providing an independent assessment of the development process and products.

Exhibit 2- 1, IV&V Iterative Feedback Process



(Showing Parallel Development and IV & V Tracks Through Implementation)

2.3.3 IV&V Team Qualifications

It is critical that the IV&V Team be able to stand “toe-to-toe” with the developers at formal reviews and walkthroughs. For this reason, it is important that the IV&V Team include senior staff with development experience equal to that of the developers with similar types of systems as the one being reviewed. In addition, to the development and IV&V experience, certifications are an invaluable tool to ensure that team members have the necessary knowledge. Some common certifications include the Certified Information Systems Auditor (CISA) and Certified Software Quality Engineer (CSQE) for IV&V, the Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) for Security, and the Project Management Professional (PMP) or comparable program management certifications. Some of these certifications can be substituted for years of experience at the discretion of the Federal Student Aid Project Manager; however, for staff with less experience, the certifications provide a level of confidence in their competency. In addition, domain knowledge and knowledge of Federal Student Aid processes, standards and systems is critical and will help minimize the learning curve required for each new system under review

2.4 IV&V Guidelines

The following section discusses those documents that the IV&V agent should apply as overarching documents when planning IV&V activities. The Lifecycle Management Framework, Enterprise Testing Standards Handbook, and relevant Federal Guidance will apply to all IV&V activities while the others are industry standards that provide a source for “Best Practices.”

2.4.1 Lifecycle Management Framework (LCM), Enterprise Testing Standards Handbook, and Work Products

The Department of Education has implemented a LCM Directive that provides a baseline for all solution acquisitions across Federal Student Aid. The LCM provides the framework to be used from the beginning stages of Planning to Retirement. The LCM Framework is based on industry best practices, standard procedures, and tools and reusable components to be used to control projects. The LCM allows Federal Student Aid personnel and contractors the flexibility to tailor these standard procedures to meet specific needs, but the LCM will not be unilaterally changed by Federal Student Aid. The use of these standard procedures will create a uniform set of expectations for all project personnel.

The Enterprise Testing Standards Handbook supports Federal Student Aid’s efforts to achieve structure, consistency, repeatability, and continuous process improvement in software testing. It sets forth policies and standards for all aspects and phases of testing, as well as the creation of the ensuing test artifacts.

In addition, Federal Student Aid has prepared a detailed Work Products Guide that defines the required deliverables during the project lifecycle.

2.4.2 Relevant Federal Guidance

The Clinger-Cohen Act of 1996 was enacted to address many of the problems related to Federal IT management. It requires Federal agencies to focus more on the results achieved through IT

investments while concurrently streamlining the IT acquisition process. This act also introduced more rigor and structure into how agencies select and manage IT projects. Among other things, the head of each agency is required to implement a process for maximizing the value of the agency's IT investments and assessing and managing the risks of its IT acquisitions.

Section 508 of the Rehabilitation Act Amendments, as amended by the Workforce Investment Act of 1998, requires that any electronic and information technology developed, procured, maintained, or used by Federal agencies will allow Federal employees and members of the public with disabilities to have access to and use of information and data that are comparable to the access to and use of information and data by Federal employees who are not disabled, unless an undue burden would be imposed on the agency. The Act allows for persons affected by it to enforce the law through the use of lawsuits. A set of accessibility standards for the Act has been published by the Architectural and Transportation Barriers Compliance Board as "Electronic and Information Technology Accessibility Standards" and applies to all acquisitions after June, 2001.

"Information Technology Investment Evaluation Guide. Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making." [GAO/AIMD-10.1.13](#) February, 1997 – recommends as part of the IT investment review process that IV&V assessments as a possible source for validating the accuracy, reliability, and completeness of systems development status information be submitted as input to the Agency IT investment cost-benefit decision making process. In addition, independently derived IV&V assessments are recommended as one possible source of ensuring that the project information is valid and that corrective actions, when necessary, have been taken.

2.4.3 Capability Maturity Model Integration (CMMI)

Capability Maturity Model Integration (CMMI) is a process improvement approach that describes the principles and practices underlying software process maturity and is intended to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. CMMI is organized into five maturity levels:

- Initial. The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.
- Repeatable. Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
- Defined. The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
- Managed. Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
- Optimizing. Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

The Capability Maturity Model Integration Acquisition Model (CMMI-AM) is a capability maturity model for organizations that acquire or procure software-intensive systems. It is used to assess their maturity and help them improve the systems acquisition process for software intensive systems. The CMMI-AM provides acquisition organizations with guidance on how to gain control of their software acquisition processes and helps them to:

- Enhance understanding of software lifecycle activities in relation to system acquisitions
- Benchmark the maturity level of the organization's acquisition process through assessment
- Improve the acquisition processes for software intensive systems
- Set senior management goals for improvement
- Enable prediction of potential acquisition process performance

2.4.4 Other Standards

ISO 9002, “Quality Management Standards and Guidelines,” is a quality assurance model, designed by the International Organization for Standardization (ISO), made up of quality system requirements. This model applies to organizations that produce, install, and service products. ISO expects organizations to apply this model, and to meet these requirements, by developing a quality system.

ISO 12207, “Software Lifecycle Processes,” offers a framework for software lifecycle processes from concept through retirement. It is especially suitable for acquisitions because it recognizes the distinct roles of acquirer and supplier. In fact, the standard is intended for two-party use where an agreement or contract defines the development, maintenance, or operation of a software system. It is not applicable to the purchase of COTS software products.

IEEE 1012-1998, “Standard for Software Verification and Validation,” provides industry standards for software verification and validation and defines the specific activities and related tasks.

2.5 Key External Organizations

The IV&V Team must account for important external organizations affecting the development process. In some cases, these organizations may clearly be outside the boundary of the project but have a major interface that requires monitoring. One such example, in the case of Federal Student Aid projects, is the Virtual Data Center (VDC).

2.5.1 Virtual Data Center (VDC)

The VDC is responsible for operational issues and has its own procedures governing these. The VDC also has important interests in issues of maintainability and configuration management related to operations. The IV&V Team will remain aware of these concerns and ensure that the developer coordinates with the VDC for any issues that cross the boundaries into operations.

2.5.2 Developer Quality Assurance

It is recommended that the IV&V Team establish an ongoing relationship with the developer's Quality Assurance Unit. IV&V must remain independent, but can still share information with the developer's Quality Assurance Unit in order to leverage each team's activities and to avoid redundancy. Regular meetings between the two teams and information sharing before major reviews are strongly encouraged.

2.5.3 CIO IT Management

The responsibility of the Chief Information Office, IT Management Group is to support Federal Student Aid's initiatives and objectives by implementing common IT components for the enterprise. The IT Management Group supports the Integrated Technical Architecture (ITA), Enterprise Service Bus (ESB), Security Architecture (SA), and the Enterprise Portal:

- **Integrated Technical Architecture (ITA).** The ITA is the integrated, enterprise wide technical architecture platform on which the Federal Student Aid applications are deployed.
- **Enterprise Service Bus (ESB).** The ESB provides dependable and controllable messaging and integration services that are essential to assist implementation and support the use of shared services.
- **Security Architecture (SA).** Security Architecture is a system consisting of IBM Tivoli Identity Manager and IBM Tivoli Access Manager (TIM and TAM) that manages access controls, provisioning, de-provisioning, self-registration, delegated administration, and simplified sign-on for multiple applications across the Federal Student Aid enterprise.
- **Enterprise Portal.** The Enterprise Portal provides one common interface/access point for end users of Federal Student Aid web applications. The Enterprise Portal will provide a different view depending on the role of the user (i.e. FSA Employee View, Student View for students, etc.).

2.5.4 Enterprise Operational Change Management (EOCM)

Enterprise Operational Change Management (EOCM) coordinates enterprise events that impact multiple Federal Student Aid systems. The CIO EOCM team tracks enterprise events and related changes as well as provides support to the Enterprise Change Control Board (ECCB). The ECCB is the Federal Student Aid Committee that is authorized to review and approve/reject enterprise changes. EOCM's role is limited to enterprise events and changes. Changes that only impact one system are handled at the system or project level and do not require EOCM involvement.

2.5.5 Other Organizations

The IV&V Team should identify all outside organizations that have a significant impact on the development process and identify the interfaces between these organizations and the development environment. The IV&V Team should then monitor these interfaces to ensure that necessary coordination between the development team and the external organization is carried out appropriately.

2.6 Standards for IV&V Activities

The IV&V Team will perform IV&V by examining the correctness, completeness, reliability, and maintainability of Federal Student Aid system products at each step in the development process. Correctness means the product being evaluated satisfies all system specification requirements. Completeness signifies all required functions are implemented and all necessary products are developed to fully support the program lifecycle. Reliability indicates the final product can be expected to perform its intended function without error or failure. Maintainability requires that the developed program products be designed to facilitate and simplify lifecycle maintenance and modifications.

The IV&V Team will assess the target system based on the type of system model (e.g., web-based or local area network (LAN)-based) and the current development schedule status. For example, in “new” target systems, the IV&V Team may concentrate upon the development phases preceding system testing. These include requirements traceability and software design analysis. The IV&V Team will provide advice on the implementation of new software technologies, perform process assessments, and resolve software issues as directed by Federal Student Aid. During testing, the IV&V Team will monitor the developer’s acceptance testing, in addition to providing an independent testing assessment. Standards for IV&V tasks are described in the following sections.

Mandatory IV&V tasks are shown in Exhibit 2-2, and Optional IV&V tasks are shown in Exhibit 2-3. The list in Exhibit 2-3 is illustrative and not exhaustive. Suggested applications for these optional tasks are provided within the exhibit. Descriptions of these optional tasks are provided in Section 2.5.12. The specific IV&V procedures to implement these tasks are detailed in Section 3.

Exhibit 2- 2, Mandatory IV&V Tasks

LCM STAGES						
TASKS BY SECTION NUMBER	Vision	Definition	Construction & Validation	Implementation	Support & Improvement	Retirement
2.5.11 Anomaly and Proposed Change Evaluation			•	•	•	
2.5.5 Independent Testing		•	•			
2.5.10 In Process Reviews	•	•	•	•	•	•
2.5.6 Metrics Analysis		•	•	•	•	•
2.5.4 Monitor System Development and Test						
--Requirements Validation	•	•	•			
--Interface Analysis		•	•			
--Design Evaluation		•	•			

LCM STAGES						
TASKS BY SECTION NUMBER	Vision	Definition	Construction & Validation	Implementation	Support & Improvement	Retirement
--Test Evaluation			•	•		
--Traceability Analysis		•	•			
2.5.8 Periodic Reviews		•	•	•		
2.5.9 Process Assessment Activities	•	•	•	•	•	
2.5.3 Product Assessment Activities	•	•	•	•	•	
2.5.1 Risk Analysis	•	•	•	•		•
2.5.7 Special Engineering Studies	•	•	•	•	•	•
2.5.2 Verify Entrance/Exit Criteria	•	•	•	•	•	

Exhibit 2- 3, Optional IV&V Tasks

LCM STAGES							
TASKS	Vision	Definition	Construction & Validation	Implementation	Support & Improvement	Retirement	CONSIDERATIONS
Additional Metrics Analysis		•	•	•	•	•	Requirements not well-defined; changing environment
Algorithm Analysis		•	•				Numerical and scientific software using critical equations or models; regulatory compliance
Control-Flow Analysis		•	•				Complex, real-time software
Database Analysis		•	•				Large database applications; if logic is stored as parameters
Dataflow Analysis		•	•	•			Data-driven real-time systems
Feasibility Study Evaluation	•			•		•	High-risk software using new technology or concepts
Functional Configuration Review			•	•		•	For large software developments

LCM STAGES							
TASKS	Vision	Definition	Construction & Validation	Implementation	Support & Improvement	Retirement	CONSIDERATIONS
Independent Regression Testing		•	•	•			Large, complex systems
Installation Configuration Review				•			Medium to large development efforts
Performance Monitoring				•	•		
Physical Configuration Review				•		•	For large software developments
Simulation Analysis	•	•	•	•			No system test capability or the need to preview the concept of feasibility or the requirements for accuracy
Sizing and Timing Analysis		•	•				
Test Certification			•	•			For critical software
User Documentation Evaluation	•	•	•	•	•	•	Interactive software requiring user inputs
Walkthroughs							
--Requirements		•					
--Design		•	•				
--Source Code			•				

2.6.1 Risk Analysis

The IV&V Team will assess the target system functions for criticality and risk. Criticality analysis will be based on the potential consequences associated with an error in or failure of the function. Risk assessment will be based on the likelihood of an error in or failure of the function. The IV&V Team will document the assessment rationale and rank both criticality and risk. The results of this analysis will be used to identify catastrophic, critical, and high-risk functions and to focus IV&V resources on the most critical aspects of the system design.

Risk management is a continuous process used to identify, quantify, and monitor risks during each stage of the LCM. The IV&V Team will verify and validate proposed approaches for reducing technical, schedule, and cost risks. The IV&V Team will also perform continuous technical and programmatic risk analysis of Federal Student Aid new projects and upgrades. At each major milestone, the IV&V Team will perform a formal risk analysis, while conducting

brainstorming sessions to review and rank potential risks to the program, and highlighting those requiring immediate attention. The IV&V Team will also assist in the preparation of risk mitigation plans, track progress towards abatement, and assist in technical and programmatic issue resolution as tasked by the Federal Student Aid Program Office. The Risk Watch List is used to track project risks and provide feedback to the developer and Federal Student Aid. This formal process will:

- Identify issues that are project risks
- Keep all identified risks easily visible at all times, rather than just those risks that are high profile at any given time
- Encourage the creation of strategies to keep risks from negatively impacting the project
- Track the risks to determine if the risk exposure changes with time
- Track the risks to ensure they are addressed
- Provide a framework for future improvement

A sample of the Risk Watch List is provided in Appendix D.

2.6.2 Verify Entrance/Exit Criteria

One of the key responsibilities of the IV&V Team will be verifying the entrance and exit criteria for each software stage or iteration, at the beginning or end of a milestone, and In Process Reviews. One of the exit criteria for each stage requires a plan for the successive stage, and the IV&V Team will review this plan to ensure that it meets the entrance criteria for the next development stage. The IV&V Team will analyze the successive stages in the development for correctness, consistency, completeness (sufficient detail to show compliance), and accuracy. All activities must meet the Department of Education approved entrance/exit criteria before proceeding to the next activity. This activity is discussed further for each lifecycle phase in Section 3.

2.6.3 Product Assessment Activities

The IV&V Team will review the target system documentation to assess the degree to which the documents meet system requirements. The IV&V Team will review phase or iteration dependent documentation using guidelines (i.e., checklists) for internal consistency, technical adequacy (e.g., requirements are unambiguous and testable), completeness, traceability to and consistency with higher level documentation, feasibility, and appropriate level of detail. As a minimum, the IV&V Team will evaluate planning, requirements, design, and test products. Optional tasks may include the review of selected code and/or user documentation.

The IV&V reviewer will be familiar with the appropriate checklists and referenced contract and standards materials before commencing the review. As the product is examined, deviations, deficiencies, and errors will be documented on a comment form (see “IV&V Reporting Standards and Procedures”) and keyed to the associated quality evaluation criteria. The reviewer will prioritize comments on a scale from 1 to 8 where a value of 1 indicates a comment that requires immediate resolution and a value of 8 indicates a typographical error, spelling or minor word change. See Section 3 and Appendix C for a discussion of specific stage-dependent procedures and the specific checklists to be applied. In some cases where a Federal Student Aid

comment form is tailored to meet the developer's needs, the priority scale can be adapted to meet their needs, e.g. high, medium, and low.

The following paragraphs provide a definition for each of the evaluation criteria appearing in the checklists. For convenience, the explanations use the word "document" for the item being evaluated, even though in some instances the item being evaluated may be something other than a document. In cases where the criteria are subjective, general guidance is provided for making the evaluation.

Adherence to Required Format and Documentation Standards. The required format for a document will be defined by Federal Student Aid approved formats, developer approved formats, and/or special contract-specified formats. Evaluation with respect to this criterion will consider whether: (1) all required paragraphs are included, (2) all paragraphs are in the required order, (3) each paragraph contains the required content, and (4) the product adheres to requirements regarding formatting, figure placement, and other presentation issues.

Compliance with Contractual Requirements. Contractual requirements are cited in the Statement of Work (SOW), Contract Data Requirements List (CDRL), the text of the contract, applicable higher level specifications, and standards and specifications included by reference in the contract. These sources will be used in evaluating against this criterion.

Internal Consistency. Internal consistency means that the document being evaluated does not contradict itself in either content or style. Elements of consistency are: (1) all statements must be compatible, (2) a given term must mean the same thing throughout, (3) a given item or concept must be referred to by the same name or description throughout, and (4) the level of detail and presentation style must be the same throughout.

Understandability. Understandability is a subjective, yet critical, component of quality. It means that: (1) the document is written using generally accepted rules of grammar, capitalization, punctuation, symbols, and notation, (2) non-standard terms, phrases, acronyms, and abbreviations are defined, (3) the material being presented can be interpreted in only one way, and (4) illustrations are adequately explained.

Technical Adequacy. Technical adequacy criterion covers the following: (1) Is the overall approach sound? (2) Does the information in the document violate known facts or principles? (3) Is it consistent with approaches known to be successful on other projects? (4) Is it well researched or based on proven prototypes? (5) Does the document appear well thought out? (6) Does the approach make sense both technically and practically?

Appropriate Degree of Completeness. Completeness means that all constituent parts are present and that each part is addressed in adequate detail. Because quality evaluations are in-process reviews, they look at products with varying degrees of completeness. The evaluator will judge whether the degree of completeness at a particular time is adequate. Sources for making this determination include project schedules, software development plans, statements indicating whether the document is preliminary or final, and common sense regarding the document's place in the overall development project. At every stage, all required paragraph titles should be present. Completeness of paragraph content

depends upon when the required information is, or should be, known based upon the product status as discussed above.

Traceability to Indicated Documents. Traceability means that the document in question is in agreement with a predecessor to which it has a hierarchical relationship.

Traceability has three elements: (1) the document in question fully implements the applicable stipulations of the predecessor document, (2) all material in the successor has its basis in the predecessor document, that is, no untraceable material has been introduced, and (3) the two documents do not contradict one another.

Consistency with Indicated Documents. Consistency between documents means that two or more documents that are not hierarchically related are free from contradictions with one another. Elements of consistency are: (1) all statements must be compatible, (2) a given term must mean the same thing in each, and (3) a given item or concept must be referred to by the same name or description in each document.

Feasibility. Feasibility is the degree to which the design stated in a document can be implemented given the state of the art, schedule and resource constraints, available tools and techniques, and other factors affecting the target system development. An additional consideration is that items that are feasible in isolation may not be feasible when taken together.

Appropriate Requirement Analysis, Design, Coding Techniques Used to Prepare Item.

This assessment will be based on industry accepted software engineering practices, the SOW, and the development agent's software development plan. This evaluation criterion is directly related to other criteria (e.g., conformance with contractual requirements) and provides the basis for determining the soundness of the engineering techniques performed during the development effort.

This evaluation criterion has a direct impact upon the criteria of technical adequacy, feasibility, and resource allocation. In cases where a comment questions the appropriateness of requirements or design analysis in one of the above noted criteria, the comment will be directed to one of the three criteria categories above. Objective evidence (e.g., the results of analysis, simulation, or modeling) will be requested to support the final evaluation of the deficiency noted in the comment.

Appropriate Level of Detail. Level of detail is a subjective criterion whose evaluation is based on the intended use of the document. A document can err in either direction: a document that is supposed to provide requirements might be so detailed as to contain design data; a document that is supposed to provide detailed design might be too high-level. Review of the applicable documentation standards and of other documents of the same type will be used to determine whether the level of detail is appropriate.

Adequate Test Coverage of Requirements. This criterion applies to test planning documents. Aspects to be considered are: (1) Is every requirement addressed by at least one test? (2) Have test suites been selected for an "average" situation as well as for "boundary" situations such as minimum and maximum values? (3) Have "stress" cases been selected, such as out-of-bounds values? (4) Have meaningful combinations of inputs been selected?

Adequacy of Planned Tools, Facilities, Procedures, Methods and Resources. This criterion applies to manuals and planning documents. The evaluation will judge as to whether the planned items will be adequate to fulfill their intended purpose.

Appropriate Content for Intended Audience. Each document has an intended audience and must be evaluated according to how well it addresses the needs of that audience. A system user, for example, does not need design details; however, those same details are critical for software support personnel. The applicable documentation standard will provide guidance for making this decision. Within the guidance provided by the documentation standard, however, a judgment will be made as to whether the material provided is suitable for the intended audience.

Testability of Requirements. A requirement is considered to be testable if an objective, feasible test can be designed to determine whether the requirement is met by the software. The requirements must be standalone and be compared against the expected results from the test. Compound requirements or vague requirements are difficult to test and should be avoided.

Consistency Between Data Definition and Data Use. This criterion applies primarily to design documents. It refers to the fact that the way in which a data element is defined should match the way that it is used in the software logic.

Adequacy of Test Descriptions/Procedures (Test Inputs, Expected Results, Evaluation Criteria). Test suites and test procedures should be sufficiently clear and specific that a person (other than the author of the test suites or procedure) could execute the test and judge unambiguously whether the evaluation criteria have been satisfied.

Completeness of Testing. Testing is complete if all test suites and all test procedures have been carried out, and all results have been fully recorded, analyzed, and reported.

Adequacy of Retesting. Retesting consists of repeating a subset of the test suites and test procedures after software corrections have been made to correct problems found in previous testing. Retesting is adequate if: (1) all test suites and test procedures that revealed problems in the previous testing have been repeated and the results have met acceptance criteria, and (2) a selected subset of the test suites and test procedures that revealed no problems during the previous testing, but that are needed to evaluate continued correct operation of the modified software, have been repeated and the results have met acceptance criteria. Criterion 1 is straightforward to evaluate. Criterion 2 is subjective. Complete retesting, using all test suites and all test procedures, is not often practical. A judgment will be made as to: (1) are the selected test suites and procedures those most likely to have been affected by the software changes, and (2) are the selected test suites and procedures those whose outcome is most important? These will be the primary criteria for judging the adequacy of retesting.

2.6.4 Monitor System Development and Test

This task includes the overall assessment of the target system requirements, design and test. Specific tasks for each of these LCM Stages are described in Section 3. The IV&V Team will perform analyses to ensure that the requirements form a solid basis for design. These analyses include requirements traceability to both the system design and test, as well as interface

definition assessments. The architecture design as well as prototype efforts (e.g., Human Computer Interface) may be assessed by the IV&V Team. As an optional task, the IV&V Team may perform analysis of appropriate sections (e.g., those deemed to be “critical”) of the source code to verify correct, complete and accurate implementation of the software requirements and design specifications and will assess the maintainability and reliability of the code.

The IV&V Team will analyze the Test Services contractor’s test program to assess complete and adequate test coverage; validity of the test definition; proper acceptance criteria; sufficient planning of tools, facilities, procedures, methods and resources; adequate planning for regression testing; and correct and complete traceability with test documents. The IV&V Team will analyze the test documentation to verify that the requirements are correctly and completely addressed and trace to all of the specified requirements. The IV&V Team may recommend specific changes to the test plans and procedures whenever defects are identified. The IV&V Team may recommend selected test scenarios to be monitored and specific test results to be independently analyzed. The IV&V Team will assess the results of formal testing of requirements and any issues or problems resulting from the verification. The IV&V Team will witness developer testing of the target system as directed by Federal Student Aid. The IV&V Team will observe testing to confirm that the tests are conducted in accordance with approved test plans and procedures.

2.6.5 Independent Testing

The IV&V Team may perform an independent test assessment of the target system as directed by Federal Student Aid. The IV&V Team will generate the test plan, test design, test suites, and test procedures in preparation for IV&V testing. The IV&V Team will perform independent testing to validate that the target system meets its critical requirements. This independent testing will complement rather than duplicate the developer’s testing.

The IV&V Team will provide the results of independent testing to Federal Student Aid, as well as to the developer. The IV&V Team will submit reports to the developer of any anomalies detected during independent testing. These incident reports should be entered by the developer into the developer’s configuration management system and also tracked independently by the IV&V Team to closure. Upon resolution of the anomaly, the IV&V Team will monitor the implementation and retesting of the fix. The IV&V Team may perform independent regression testing as an optional task.

2.6.6 Metrics Analysis

The IV&V Team will use software metrics in predicting the target system’s ability to comply with requirements and schedules. The IV&V Team will review proposed software progress and quality metrics for conformance to sound software engineering principles as well as to Department of Education reporting requirements. Some of the technical metrics may include software development and test schedule metrics, and software error reporting. Additional metrics analysis tasks are discussed in Section 2.5.12 and Section 6.

2.6.7 Special Studies

Throughout a project's development, technical and programmatic issues may arise that require special studies to resolve. For each issue selected for analysis, the IV&V Team will prepare a

brief plan and submit the plan to the Federal Student Aid Program Manager for approval prior to initiating the analysis. In addition to proposed activities, schedule, travel requirements, estimates of effort, and impact upon other tasks (if any), each plan will include:

- The exact nature of the problem to be analyzed along with all available detail
- The goal of the special study or investigation (for example, to determine the source of the problem or to create evaluation models)
- The ground rules for conducting the special study or investigation (for example, security considerations, degree of interference with the development agent allowable, and/or roles of other agencies)
- The time frame allowed for completion of the effort

Following the completion of each analysis, the IV&V Team will submit a report to the Federal Student Aid Program Manager that summarizes the analysis, findings, and conclusions and highlights any follow-up activities that are required to enable final issue resolution.

2.6.8 Periodic Reviews

The IV&V Team will perform system-related process and product reviews at the developer's sites throughout the LCM. These process and product reviews will be scheduled through the Federal Student Aid Quality Assurance (QA) Program Office and coordinated with the developer's schedule. The process review will search for objective evidence that the developer is following the appropriate development plan. The product review will concentrate on the actual software development artifacts that represent the system at that point in its development.

2.6.9 Process Assessment Activities

The IV&V Team will assess the developer's software processes using multiple criteria including statements-of-work, Department of Education standards, and the developer's plans and policies. The IV&V Team will assess the developer's process infrastructure, which may include software development plans and the establishment of a software engineering environment. The IV&V Team will evaluate the developer's proposed use of commercial and/or custom software development/test tools.

CMMI will be the standard for assessing and recommending improvements for the developer's software processes. This model is an effective means for modeling, defining, and measuring the maturity of the processes used during software development. See Section 2.4.3 for more information on the levels of CMMI.

Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. The IV&V Team will use CMMI to identify the key practices that are required to increase the maturity of the developer's software processes. Except for Level 1, each maturity level is decomposed into several key process areas that indicate the areas an organization should focus on to improve its software process. Each key process area is described in terms of the key practices that contribute to satisfying its goals. The key practices describe the infrastructure and activities that contribute most to the effective implementation and institutionalization of the key process area.

The IV&V Team will initially focus on Maturity Level 2 or the level that the Development Services or Testing Services contractor has attained, whichever is higher. CMMI Level 2 addresses the software project's concerns related to establishing basic project management controls.

The IV&V Team should also target their reviews based on the CMMI level the development organization has attained. The key process areas are Requirements Management, Software Project Planning, Software Project Tracking and Oversight, Software Subcontractor Management, Software Quality Assurance, and Software Configuration Management. Goals will be updated as each maturity level is attained.

The IV&V Team will assess the developer's configuration management organization. The IV&V Team will monitor the configuration management activities of configuration identification, configuration control, and configuration status accounting and reporting. The IV&V Team may perform configuration control reviews to assess the developer's configuration control procedures and the enforcement of these procedures. If available, the IV&V Team will review the developer's formal configuration management plan. The IV&V Team will evaluate the developer's configuration management tools and methodologies.

2.6.10 In Process Reviews

In Process Reviews (IPRs) will be conducted during the development process to keep the community apprised of Federal Student Aid program development status. Federal Student Aid (and perhaps other Department of Education organizations), the developers, and the IV&V Team participate in these meetings. The IV&V Team will review Federal Student Aid-defined entrance and exit criteria for these reviews to insure that all goals are met and that the developer can proceed with the next phase of development. These reviews may be in the form of System Requirements Reviews, Design Reviews, or Readiness Reviews. In addition, the IV&V Team will provide a quarterly IPR as required by the contract that includes Accomplishments, Upcoming Activities, Issues and Risks. Participants will include IV&V, Enterprise Quality Assurance, the Federal Student Aid Project Technical Leads and System Managers, the System Security Officer, and, at the discretion of Federal Student Aid, a representative from the development team. The IV&V Team will also provide the results of applicable IV&V tasks to support these reviews. In addition, as directed by Federal Student Aid, the IV&V Team will support Post Implementation Reviews to assess the operation and maintenance of the target system, as well as evaluate the "Lessons Learned" as a result of the overall development.

2.6.11 Anomaly and Proposed Change Evaluation

The IV&V Team will monitor the status of target system anomalies (also known as incidents) and deficiencies to assure the validity of any resultant changes. The IV&V Team will monitor anomalies detected during both developer and independent testing. These will be tracked and trend analyses may be performed to determine the number of test-related problems. If requested by Federal Student Aid, the IV&V Team will review any software defects discovered (or outstanding) after completion of target system testing. The IV&V Team will review corrective actions, verify priorities and confirm the disposition of the change. The IV&V Team will perform detailed reviews of the anomalies to help verify the correct disposition of system problems. If tasked by Federal Student Aid, the IV&V Team will participate in the regression

testing of the fixes. In addition, the IV&V Team will support Configuration Control Boards (CCB) if requested by Federal Student Aid and provide inputs as needed.

The IV&V Team will also review proposed change candidates initiated when a revision to the baseline requirements is necessary to enhance or improve the program's function. If tasked by Federal Student Aid, the IV&V Team will participate in functional working groups to define system and software upgrade requirements. For this optional task, the IV&V Team will perform requirements analysis including the development of technical reports, desktop analyses, and coordination of community inputs. The IV&V Team will review these proposed requirements for feasibility, accuracy, and completeness, while assessing the impact on the operational system.

As part of the anomaly and proposed change assessment, the IV&V Team will perform some or all of the following:

- Perform independent impact assessments concerning the expected operational environment, affected interfaces, feasibility, technical approach, and testability
- Provide evaluation of risks
- Conduct independent reviews of proposed changes as required
- Perform traceability analyses to ensure that all affected documents accurately, correctly, and consistently reflect the approved changes
- Conduct an independent review of the resulting design
- Monitor the implementation progress and review code to detect development problems and/or unapproved deviations
- Monitor regression testing to validate incorporated system changes

2.6.12 Optional IV&V Tasks

Optional IV&V Tasks will be performed at the discretion of the IV&V Team and Federal Student Aid. By selecting IV&V's recommendations from these optional IV&V tasks, the IV&V Team can tailor the IV&V effort to Federal Student Aid needs and also achieve a more effective IV&V effort.

Additional Metrics Analysis. The IV&V Team will prepare a metrics analysis report for Federal Student Aid which summarizes the developer's metrics, presents the results of the IV&V Team analysis (both objective and subjective), and provides conclusions and recommendations to Federal Student Aid. For example, the developer's metrics report may include raw data such as development status, object integration status, system test status, test anomaly status, source lines of code (SLOC) count, simulation status, staffing, and development schedule. The IV&V Team will assess the developer's progress to date, progress since last period, progress versus planned, work units remaining, and ratio of incremental accomplishment to that required to complete on schedule. The IV&V Team will retain the original plans for schedule, rate of accomplishment, and original SLOC estimates so that current status may be measured against planned status.

Algorithm Analysis. The IV&V Team will confirm that selected algorithms are correct, appropriate, and stable, and meet all accuracy, timing and sizing requirements.

Control Flow Analysis. The IV&V Team will confirm that the proposed control flow is free of problems, such as design or code elements that are unreachable or incorrect.

Database Analysis. The IV&V Team will confirm that the database structure and access methods are compatible with the logical design.

Data Flow Analysis. The IV&V Team will confirm that the input and output data and their formats are properly defined, and that the data flows are correct.

Feasibility Study Evaluation. The IV&V Team will evaluate feasibility studies performed during the Concept Design for correctness, completeness, consistency, and accuracy. The IV&V Team will trace back to the statement of need for the user requirements. Where appropriate, the IV&V Team will conduct an independent feasibility study as part of the IV&V tasks.

Functional Configuration Review. Prior to delivery, the IV&V Team will assess the performance of the software relative to the requirements specified in the software requirements specifications.

Independent Regression Testing. The IV&V Team will independently determine the extent of IV&V analysis and independent testing that should be repeated when changes are made to any software products previously examined.

Installation Configuration Review. The IV&V Team will perform an installation configuration review to assess the operations with site dependencies and the adequacy of the installation procedure.

Performance Monitoring. The IV&V Team will collect information on the performance of the software under operational conditions. The IV&V Team will determine whether system and software performance requirements are satisfied.

Physical Configuration Review. The IV&V Team will assess the internal consistency of the software, its documentation, and its readiness for delivery.

Simulation Analysis. The IV&V Team will simulate critical aspects of the software or system environment to analyze logical or performance characteristics that would not be practical to analyze manually.

Sizing and Timing Analysis. The IV&V Team will obtain program sizing and execution timing information to determine whether the total of the allocated budgets is within the overall allocation for the item. Analyses should include network resources (bandwidth, servers, etc.). More subtle assessments include: (1) Do the allocations seem realistic and feasible? (2) Do they take into account the demands on each computing unit or component, or do they seem to be more mechanical allocations, such as dividing available storage by number of computing units? (3) Are they based on prototyping and other analysis, or just on guesswork? (4) Are they worst case? (5) Do they allow for the reserve requirements?

Test Certification. The IV&V Team will confirm that reported test results are the actual findings of the tests. Test related tools, media, and documentation will be certified to confirm maintainability and repeatability of tests. This may be performed informally or as part of the optional Functional Configuration Review.

User Documentation Evaluation. The IV&V Team will examine draft documents during the development process to confirm correctness, understandability, and completeness. Documentation may include user manuals or guides, as appropriate for the project.

Walkthrough. The IV&V Team will participate in the evaluation processes in which development personnel lead others through a structured examination of a product. The IV&V Team will assess the developer's review process, product checklists, defined roles of participants, and forms and reports. The IV&V Team will observe if the walkthrough process is well-structured, and if issues and action items are recorded and progress monitored. The specific types of walkthroughs that the IV&V Team may assess include requirements walkthroughs, walkthroughs of the preliminary design and updates of the design, and source code walkthroughs.

2.7 IV&V Tools

To perform effective IV&V, the IV&V Team will employ an integrated IV&V toolset that may include requirements, design and code analysis, test, and metrics tools. The objective of the tools is to enable more efficient and accurate verification and validation of design, code, and test documentation. However, it must be recognized that tools do not replace analysis by qualified engineers. The team will select tools based on established IV&V program goals, organizational compatibility, tool effectiveness, solution constraints, cost, acquisition time requirements, and training requirements. COTS tools will be selected wherever possible. Federal Student Aid has adopted the Rational Tool Suite and this tool is used by many of the developers as well. This includes Requisite Pro for requirements analysis, ClearCase for configuration management, and ClearQuest for defect tracking. It is recommended that the IV&V Team be somewhat experienced in the use of these tools, as access to these tools may be required to review many of the development artifacts. If required to support IV&V analyses, the IV&V Team will also develop automated tools or modify existing ones through custom programming solutions or COTS scripts per direction from the Federal Student Aid Program Manager.

2.7.1 Computer Aided Software Engineering (CASE) Tools

CASE Tools provide the software developer with a complete set of visual modeling tools for development of software in the client/server, distributed enterprise and real-time systems environments. If access is provided, the IV&V Team will use these design tools in performing on-site reviews of Software Development Files (SDF) or Application Folders and perform technical analysis of design information. When the IV&V Team is not on-site at the developer's facility, the IV&V Team will review the design reports, models and output from the CASE tool.

2.7.2 Requirements Management Tools

Requirements Management Tools provide a mechanism for tracking the requirements traceability through design, code, and testing. These tools help to verify that all requirements are successfully incorporated into the system development and tested. The IV&V Team will use the developer requirements management tools whenever possible to monitor the requirements and the associated traceability. When off-site at the IV&V Team's offices, the IV&V Team may have web based "read-only" access to the requirements database or may request (or require) regular snapshots of the requirements database to perform various traceability tasks. In addition, the

IV&V Team may use additional tools to import some of the requirements to perform various reviews and traceability activities. Lastly, the templates provided in Appendix E provide mechanisms for tracking the developer's traceability activities.

2.7.3 Configuration Management Tools

The IV&V Team will analyze the developer's configuration management tool suite to verify that requirements and source code are under configuration control. The developer may use several configuration management tools as appropriate to its various software development environments; however, it is strongly recommended that the developer implement a standard tool for consistency. The IV&V Team will confirm that each tool provides an environment wherein all change management is handled consistently. This promotes uniformity across the team and minimizes errors.

2.7.4 Test Tools

The IV&V Team will examine the developer's test tools (e.g., test generation tools) used for Unit, Integration, System, UAT and Post Implementation Verification. Acceptance Testing for some of the target systems may be performed using automated test scripts to exercise the system. The IV&V Team will verify the correct execution of these scripts during testing and will verify the test outputs from these tools.

2.7.5 Model Verification and Analysis Tools

The IV&V Team may review, verify and validate computerized system and performance models, if available. Models will be evaluated for viability to satisfy requirements and validated for consistency with the system architecture, concept of operations and evolving designs. At a minimum, modeling techniques, methodologies, tools and checklists will be documented and expected results will be verified. The IV&V Team will review these models and verify their feasibility and correctness.

The IV&V Team will have software lifecycle cost estimation tools to analyze and validate the software sizing and cost estimates provided by the developer. As requested, the IV&V Team will support the Federal Student Aid Program Office in preparation for independent cost estimates using Constructive Cost Model (COCOMO), Revised Intermediate COCOMO, or other analysis tools. The IV&V Team will calibrate these tools with historical data from previous upgrades combined with analyses of any new requirements. The IV&V Team may also use tools and various compilers to analyze the source code and verify SLOC estimates. Specific tools will be selected and documented, as required.

2.8 IV&V Engagement and Tailoring Strategies

Federal Student Aid target systems cover a broad range of disciplines, staff sizes, types of efforts, developments, and duration. Therefore, the IV&V lifecycle analysis tasks must be tailored to match the tools and unique processes inherent in the applicable methodology and development environment. The specific IV&V tasks detailed in these standards and procedures are in accordance with the applicable software development lifecycle stages described in the LCM. Section 3 of these standards and procedures addresses each of these phases in detail.

Throughout the development lifecycle phases, the IV&V Team conducts IV&V of all system modifications, enhancements, additions, and approved changes.

The IV&V plan for a specific project should be tailored for the chosen development environment. The major factors IV&V will consider are lifecycle methodology, traditional versus accelerated development, centralized versus Internet development environment, and externally imposed constraints. It must be kept in mind that key development issues such as requirements always remain important; the only differences may be in the timing and methods used, not whether or not they will be evaluated in depth.

2.8.1 Lifecycles

A lifecycle model is a plan that outlines the way in which a project is to perform the activities central to that project. A software methodology is a more detailed expression of this plan that follows certain established software engineering principles. It also establishes the criteria used to determine if it is appropriate to proceed from one task to another. The LCM Directive does not dictate the particular methodology to be used but allows the developer to use one that is appropriate to the project as long as it satisfies the guidelines of the LCM. The following section outlines the IV&V strategies appropriate to specific methodologies. These should be considered as a general guide only, since it is impossible to authoritatively state that one method will always be better than another. The differences between the methods are often not as clear as the descriptions make them appear, as developers and managers may mix these approaches at some levels. These matrices highlight those IV&V functions that should receive particular emphasis, but it should be noted that all IV&V functions remain important, and none should be neglected.

2.8.2 Waterfall

In this model, the oldest and still one of most commonly used, the project proceeds through a series of separate sequential steps starting with the concept and ending with implementation. There is usually a review at the end of each step to determine if it is acceptable to proceed to the next step. If it is found that the project is not ready to proceed, the project is held in the current step until it is ready. In the pure form of this methodology, the different steps do not overlap.

Table 2- 1, Waterfall

Characteristics	IV&V Response
Well-defined, sequential stages characterized by clear entry/exit criteria.	Conduct review of entry/exit criteria at boundary between stages and ensure that stage is finished.
Requires clear and complete documentation for each stage.	Ensure that documentation is clear and complete at exit from each stage.
Development team should be very familiar with technical methodologies used.	Ascertain in Vision Stage that team is experienced in tools selected for project.
Requires knowledgeable users with in-depth knowledge of system and a commitment to provide developer with support to define requirements.	Ensure that developer identifies key customers and conducts in-depth review sessions, Joint Application Design (JADs) to define requirements. Ascertain if developer is receiving required support from

Characteristics	IV&V Response
	key customers with appropriate knowledge.
Requires detailed definition of requirements prior to Construction Stage.	Ensure that requirements are sufficiently detailed before exit from Definition Stage.
Software delivered at the end of the project, so progress may not be clear.	Closely monitor the Project Work Plan and ensure that any project slippage is reported.

Modified Waterfalls

There are different versions of this method but they may approach the problem by modifying the traditional "pure" waterfall approach by allowing the steps to overlap, reducing the documentation, and allowing more regression. Some of the more useful versions are described in the following sections.

Overlapping Waterfalls

The development stages overlap allowing discovery and insight in later stages; i.e., the requirements analysis may still be occurring partway into the Detailed Design stage. This mirrors many real-life projects.

Table 2- 2, Overlapping Waterfall

Characteristics	IV&V Response
Documentation may be reduced during intermediate stages if continuity of personnel is maintained.	If personnel turnover becomes high or key personnel leave, IV&V shall review documentation and highlight areas of uncertainty.
Requirements will probably not be completely defined until the Build portion of the Construction Stage.	Monitor Requirements Traceability Matrix (RTM) closely to identify open requirements, partially defined requirements, and requirements not defined to appropriate level of detail. If they are not addressed at a determined point in the Construction Stage, identify them as high risk issues.
Requirements may change late in cycle.	Ensure that changes are tracked through the CM process and that all affected code is regression tested. This may include sections of code not changed but interacting with changed code.
Milestones are more ambiguous because the clear boundary between stages is no longer available.	Review Project Work Plan for clear points at which progress can be checked. Monitor checkpoints and quickly report slippage from these points.
Activities being performed in parallel can lead to miscommunication, mistaken assumptions, and inefficiency.	Review documentation, attend meetings, review meeting notes, email and other communication means, and note any areas of confusion. Alert developer and work with development team to identify areas where communication problems are increasing.

Waterfall with Subprojects

The architecture is broken into logically independent subsystems that can be done separately and integrated together later in the project. This allows each subproject to proceed at its own pace rather than having to wait for all subprojects to have reached the same stage of readiness before proceeding to the next stage.

Table 2- 3, Waterfall with Subprojects

Characteristics	IV&V Response
Architecture is broken into logically independent subsystems that can be done separately and integrated together later in the project.	Closely review subsystem definition, looking for unidentified interdependencies between subsystems.
Subsystems are integrated late in project.	Closely monitor testing after integration to ensure that relationships between subsystems are thoroughly tested.

Waterfall with Risk Reduction

A risk reduction spiral (see Spiral Development below) is introduced at the requirements stage and/or the architectural stage.

Table 2- 4, Waterfall with Risk Reduction

Characteristics	IV&V Response
Do not have to fully understand requirements before beginning architectural design.	Ensure that a thorough review of deliverables is done at the end of each spiral iteration and that they are correct for the objectives defined at the beginning of the spiral.
Complicates management of project.	Ensure project management is closely monitoring project issues and tracking risks. Ensure mitigating strategies are identified for project risks.

2.8.3 Prototyping

The system concept is developed as the development team moves through the project by developing and demonstrating part of the system, usually the most visible part, to the customer. Modifications may be made and the next part is then developed based on feedback from the customer. At some point, agreement is reached between the customer and the developer that the prototype is satisfactory and outstanding work is finished and the system delivered.

Table 2- 5, Prototyping

Characteristics	IV&V Response
Software is demonstrated to customer as it is developed and modified according to customer feedback.	Monitor for signs that project scope is growing out of bounds. There should be clear agreement at the end of each prototyping session that the system is evolving rather than simply growing. Modifications should be clearly identified and accepted by both developer and customer.
Scope of project will not be well known at beginning.	Track requirements to verify that they are being refined. If new requirements are identified, examine them to see if they will fit within the time and budget constraints of the project.
Requirements may change rapidly.	Monitor for signs that methodology is not slipping into "code and fix" mentality.

2.8.4 Spiral

This is a risk-oriented method that breaks a project into smaller "mini-projects." Each mini-project focuses on one or more identified major risks in a series of iterations until all risks have been addressed. Once all the risks have been addressed, the spiral model terminates the same way the waterfall model does.

Table 2- 6, Spiral

Characteristics	IV&V Response
Good model for many Rapid Application Development (RAD) projects.	In Vision Stage, examine in terms of specific project needs and point out alternative methodologies if applicable.
Complicated and requires sophisticated, experienced management and personnel.	In Vision Stage, ensure that development team has experience in, and understanding of, the methodology.
Iterative, risk-oriented model.	<p>Make certain iterations start on a small scale and build in importance. Ensure objectives, risks, and deliverables are all clearly identified in each iteration.</p> <p>Ensure risk-model is not used as an excuse for skipping the iteration, or iterations, necessary to establish clear requirements.</p> <p>Thoroughly examine iteration artifacts at the end of each iteration for indications that risks cannot be dealt with satisfactorily.</p>

2.8.5 Staged Delivery

This bears some similarities to both Prototyping and Waterfall with Subprojects in that software is demonstrated and delivered to the customer in successive stages. The steps up to and through architectural design are the same as the Traditional Waterfall, and the following build and deliver steps are done for each of the separate stages. It differs from Prototyping in that the scope is established at the beginning of the project and the software is delivered in stages rather than in one package at the end as is done with the waterfall method. It differs from Waterfall with

Subprojects in that the stages are delivered independently rather than integrated towards the end of the project.

Table 2- 7, Staged Delivery

Characteristics	IV&V Response
Requires careful planning from both managers and technical leads.	Review stage definitions and justification carefully to verify that chosen breakdown is credible.
Interdependencies between stages must be understood.	Review stages for unidentified interdependencies. Make sure that all stages are tested as a system after delivery of the final stage.
Customers receive useful stages before the end of the project.	Review stages as they are delivered to verify that they meet user needs and are acceptable to the customer.

2.8.6 Hybrid Approaches

These methodologies may be combined, e.g., a risk spiral combined with a modified waterfall, or prototyping with Waterfall or Spiral. However, care should be taken that this is done for the purpose of improving the development process for a particular project, not for reasons of expedience. For instance, Spiral development should not be chosen under the assumption that it lessens the need for the development of requirements. The Spiral methodology differs in the manner in which and the stage at which the requirements are determined, not whether or not the requirements are specified and documented. The tailored IV&V response to a Hybrid methodology will depend on which methodologies are used.

2.8.7 Commercial Off-The Shelf (COTS) Software

These are commercial software products developed to meet certain needs. These packages vary considerably in complexity and cost depending on the needs they are designed to meet. The nature of these products does not reduce the requirement for IV&V because they still must be integrated with other components of the target systems.

Table 2- 8, COTS Software

Characteristics	IV&V Response
Will rarely satisfy all needs, especially for large, complex systems.	In Vision Stage, carefully review capabilities of proposed software to verify that it meets minimal needs.
Immediate availability (immediacy varies depending on amount of tailoring necessary).	Determine if timetable necessary to install package will negate time gained by purchasing commercial software. Confirm by examining the experience of similar organizations.
Can be revised to meet custom needs.	Examine software capabilities in light of customer expectations to determine degree of realistic customization compared to probable customer needs for future change.

2.8.8 Rapid Application Development (RAD)

RAD is a term often used without being clearly defined. It may mean rapid prototyping to one user, the use of CASE tools and tight deadlines to another or a headline article in a trade journal to a third. As a useful term in a strategic sense, the best usable definition is that RAD means a project that requires an accelerated development environment compared to more traditional project modes and timelines. It requires more careful management and better understanding of the risks involved. Using this definition frees RAD of association with any one set of tools and focuses on the relationship between software development methods within specific environments especially in relation to time constraints.

There are no hard and fast rules regarding which methodology is best for RAD. There are some projects that can be developed more rapidly by a team coding in COBOL than by a team using an Object Oriented Development (OOD) approach because the OOD team may have to spend significant time defining and developing the underlying classes. Which approach to take in this example might hinge on risk factors comparing time constraints to the value of future code reuse in the given environment. The same factors affect the IV&V approach taken. See Exhibit 2-4 for a comparison of full IV&V with externally constrained IV&V and RAD IV&V.

2.8.9 Development Environments

IV&V needs to consider the differences between the traditional development architectures of mainframe, desktop, and client-server compared to the newer environment represented by the Internet, specifically Web-enabled applications with a large, diverse, distributed user community. The Web has given organizations unparalleled means of providing easy access to constituencies. At the same time it has introduced perspectives and problems that were not evident in the preceding technologies. The main areas of concern for IV&V in a Web environment may be categorized as:

- User base may be very large and poorly defined compared to that of a traditional system
- Wide variation in client hardware and software
- Privacy issues
- Accessibility issues as expressed in Section 508 assume even greater importance
- Usability issues
- Site navigation
- Security
- Performance issues due to larger user base and the use of images
- The graphical interface presents a public face
- Availability issues in terms of users being accustomed to 24/7 access; frustration now that perceived slow response is measured in seconds, not days or hours
- More interactive (e-mail notifications and responses)
- Online forms
- Downloadable documents

- Search engines

For these reasons, it is critically important that all Web development must meet Department of Education standards for Web development.

2.8.10 Externally Imposed Constraints

For best results, IV&V should always begin as early as possible in the lifecycle and be performed as described in this Handbook throughout the cycle. However, there are times when an abbreviated IV&V must be performed due to external constraints. IV&V efforts may be tailored for these circumstances, but it must be remembered that the level of project risk will rise substantially as the level of IV&V effort is reduced. The two most common reasons for such constraints and the corresponding tailoring strategies are described in the following two sections.

Regardless of the limitations imposed by these situations, the IV&V Team requires timely access to developer documentation, status information, requirements, CM data, test results, and anomaly data. The IV&V Team requires visibility into the development and test effort as early as possible. Access must be complete, but the effort of the IV&V Team from the point of involvement will be determined by the type of external constraint. The IV&V Team must still be exposed to all aspects of the development effort in order to perform an adequate and accurate assessment. The cooperation of the developer will become even more important in developing a good working relationship with the IV&V Team. Exhibit 2-4 compares the IV&V activities performed across three levels of effort: full IV&V, externally constrained IV&V (including constraints due to budget and delayed start of project), and RAD.

2.8.10.1 Budgetary Constraints

Tailoring of IV&V due to budget constraints dictates the approach to IV&V be a targeted one, with particular emphasis placed on establishing a benchmark set of requirements and processes early in the lifecycle to help transition to the scaled down effort of a targeted monitoring role. Risk management will be used to target the IV&V approach to those areas of greatest risk. The responsibility of the developer in producing good requirements will be increased because of the limitations on IV&V involvement.

IV&V resources will be focused on specific development activities and products that pose the highest risk to successful completion of the target system. The IV&V Plan will be tailored to utilize the limited budget for specific IV&V activities that mitigate risk on critical, high-risk development activities. Sampling of requirements and artifacts may be used, but should be based on the risk assessment and criticality analysis.

2.8.10.2 Delayed IV&V

Delayed IV&V refers to the assignment of the IV&V Team after the beginning of the LCM. Tailoring of IV&V due to delayed entry will be based on the point at which the IV&V Team enters the project. A risk assessment should be done immediately, with attention focused on the specific development activities and products that pose the highest risk to successful completion of the target system. The RTM will have to be developed primarily by the developer, and any independent tracing of requirements by the IV&V Team will be based on sampling determined by the risk assessment. The IV&V Plan will focus on testing based on major requirements and on identifying risks for the Production Readiness Review (PRR). Late entry of IV&V may be considered a sign of concern about the project and should not be considered as a means of saving

a project. At best in this situation, IV&V can provide independent information on the risks of proceeding with the project and offer strategies for mitigating those risks.

Exhibit 2- 4, Comparison of Full IV&V to RAD IV&V and Externally Constrained IV&V

Tailored Activities	Full IV&V	External Constraint IV&V: Budget	External Constraint IV&V: Delayed Start	RAD
Develop and maintain tailored IV&V/QA Plan.	✓	Update	From entry	Update
Provide Weekly Status Report and issues tracking log.	✓	✓	✓	✓
Verify Entrance/Exit Criteria for all reviews, e.g., TRR.	✓	✓	From entry	✓
Support Pre-Production Readiness Review (PRR) and prepare recommendation for PRR.	✓	✓	✓	✓
Risk analysis including preparation and maintenance of Risk Watch List.	✓	✓	✓	✓
Monitor Project Work Plan and track schedule slippage.	✓	✓	From entry	✓
Requirements review for testability and correctness.	✓	Sampling	Sampling	Sampling
Review Technical Products for correctness and maintainability.	✓		✓	
Monitor Test Activities to verify adherence to process.	✓	✓	✓	✓
Review all test scripts, results and artifacts for completeness and accuracy.	✓	Sampling	✓	✓
Prepare final end of stage reports (compilation) with lessons learned.	✓	✓	✓	✓
Review project plan for compliance.	✓	Sampling	From entry	✓
Requirements Traceability through design and test documentation to verify design and to ensure testing of correct requirements. Deliver formal RTM.	✓	Sampling	Sampling	Sampling
Process Compliance Reviews (CM, Rational etc)	✓	Sampling	Sampling from entry	Sampling

Tailored Activities	Full IV&V	External Constraint IV&V: Budget	External Constraint IV&V: Delayed Start	RAD
Perform targeted independent testing of critical or high defect areas of system as appropriate.	✓	Sampling	✓	✓

Update: Refers to periodic update of the specified product rather than continuous maintenance.

Sampling: Refers to selection and monitoring of a subset of the specified product that is believed to represent the entire set.

2.8.10.3 EDSS Phased Contract Approach

With the EDSS approach to System Acquisition, there is a possibility that the development contractor may change during different stages of the development lifecycle. For example, one contractor may be selected for the Definition Stage, while another is selected for the Construction and Validation Stage. It is recommended that IV&V be consistent throughout the lifecycle to provide a consistent presence on the project. In addition, stage gate reviews and complete documentation are critical, and it must be verified that this documentation is complete and adequate for the next phase since the subsequent development team will have no ownership or responsibility for these development products.

Section 3. Independent Verification & Validation (IV&V) Procedures

3.1 Overview

This section provides the procedures for the IV&V tasks to be performed throughout the development lifecycle. Federal Student Aid's LCM structure consists of IV&V Team activities, procedures and deliverables. Exhibit 3-1 provides a diagram of the lifecycle process and depicts the informal and formal IV&V processes and techniques employed for each stage of development. The recommended IV&V activities, which are required by the IV&V standard for each development stage, are shown in this exhibit. Lifecycle Verification and Validation includes technical procedures for verifying that products and processes of each stage of the lifecycle meet the requirements imposed by the previous stage, and for validating that the developed products comply with the original target system requirements.

3.2 Management of IV&V

The IV&V Team will perform IV&V procedures in parallel with software development. Each IV&V lifecycle stage ends when the IV&V tasks for each stage are completed and the software development products are determined to be adequate. IV&V lifecycle stages may overlap as activities of the new lifecycle stage are beginning and activities of the previous one are nearing completion. In addition, some IV&V tasks are iterative; as changes are made to the software product, selected IV&V tasks from the previous lifecycle stages will be performed again, or additional IV&V tasks will be performed to address the changes. The complexity and scope of changes determine the level of detail covered by the iteration.

As discussed in Section 2, multiple methodologies may be used in the development of Federal Student Aid systems. While this plan addresses tasks used in all of the applicable methods, the IV&V Team will address each task in the context of the methodology outlined by the LCM and supported by the Work Products Guide. The following procedures are mature and follow the standards described in Section 2. They include the mandatory as well as the optional IV&V procedures and tasks. All referenced checklists are included in Appendix C, and referenced reporting templates are in Appendix E.

3.2.1 IV&V Plan Generation

The IV&V Team will generate an IV&V Plan for all lifecycle processes. This plan will be based on the lifecycle stages and methodology defined by the LCM, to include a listing of key activities and deliverables. In addition, any unique aspects of the IV&V effort will be addressed along with any specific required tailoring. This plan will be re-evaluated at the conclusion of the IV&V effort for process improvement and for any required updates to this plan. These updates may also be applied to IV&V of the operational system as well as being captured as lessons learned. A template for this plan is included in Section 5.2.2.1.

3.2.2 Baseline Change Assessment

The IV&V Team will evaluate proposed software changes (anomaly and requirement changes) for effects on current and previously completed IV&V tasks. IV&V provides a unique perspective, taking a system view rather than a segment or element view of the system. Since the IV&V team reviews all of the documentation and attends meetings across organizations, IV&V is able to monitor and trace the impact of changes and dependencies throughout the development effort. At times, IV&V is the only party performing analysis from a system perspective. Because of this unique view, it is imperative that IV&V review changes based on the entire development picture rather than just the current stage or “hot topic.” IV&V must also assess the impacts of these changes, and provide an assessment of the impacts from both an operational and maintenance perspective. In addition, the IV&V team must ensure that the changes are reflected in updates to both current and previous stage documentation for consistency, correctness and maintenance purposes. The team will also participate in key reviews of these changes and make recommendations as appropriate.

3.2.3 Management and Technical Review Support

During key milestone activities, the IV&V Team will verify entrance and exit criteria and gather supporting evidence on whether to recommend moving on to the next set of software development activities. In addition, the IV&V team must remain flexible and be ready to adapt to any unforeseen major change in scope or process of the development effort. These changes could result in a subsequent modification to the IV&V process as long as the changes do not impact the integrity of either the IV&V or development effort.

The IV&V Team will participate in the PRR and will provide a final recommendation at the PRR. However, the team must provide targeted feedback early in the process and work with the developer to keep the lines of communication open. IV&V must adopt a “no surprises” approach and ensure there is constant communication with the development team during all stages of development. While the input at the PRR is important, IV&V will ensure issues will not surface at the PRR for the first time.

3.2.4 Interface with Organizational and Supporting Processes

The IV&V Team must coordinate with other groups that are part of the development effort to ensure information sharing of process improvements and lessons learned. These interfaces should be documented in the IV&V plan as participation and cooperation with various groups including control boards and integrated product teams. The IV&V team will continue to review their processes and procedures to find innovative ways to maximize their working relationship with developers and management, and continue to build a team-oriented approach. As discussed in Section 2.5.2, it is recommended that the IV&V Team establish an ongoing relationship with the developer’s Quality Assurance Unit. Communication and information sharing mechanisms should be established and documented in the IV&V Plan.

3.2.5 Federal Student Aid LCM and Work Products Guide

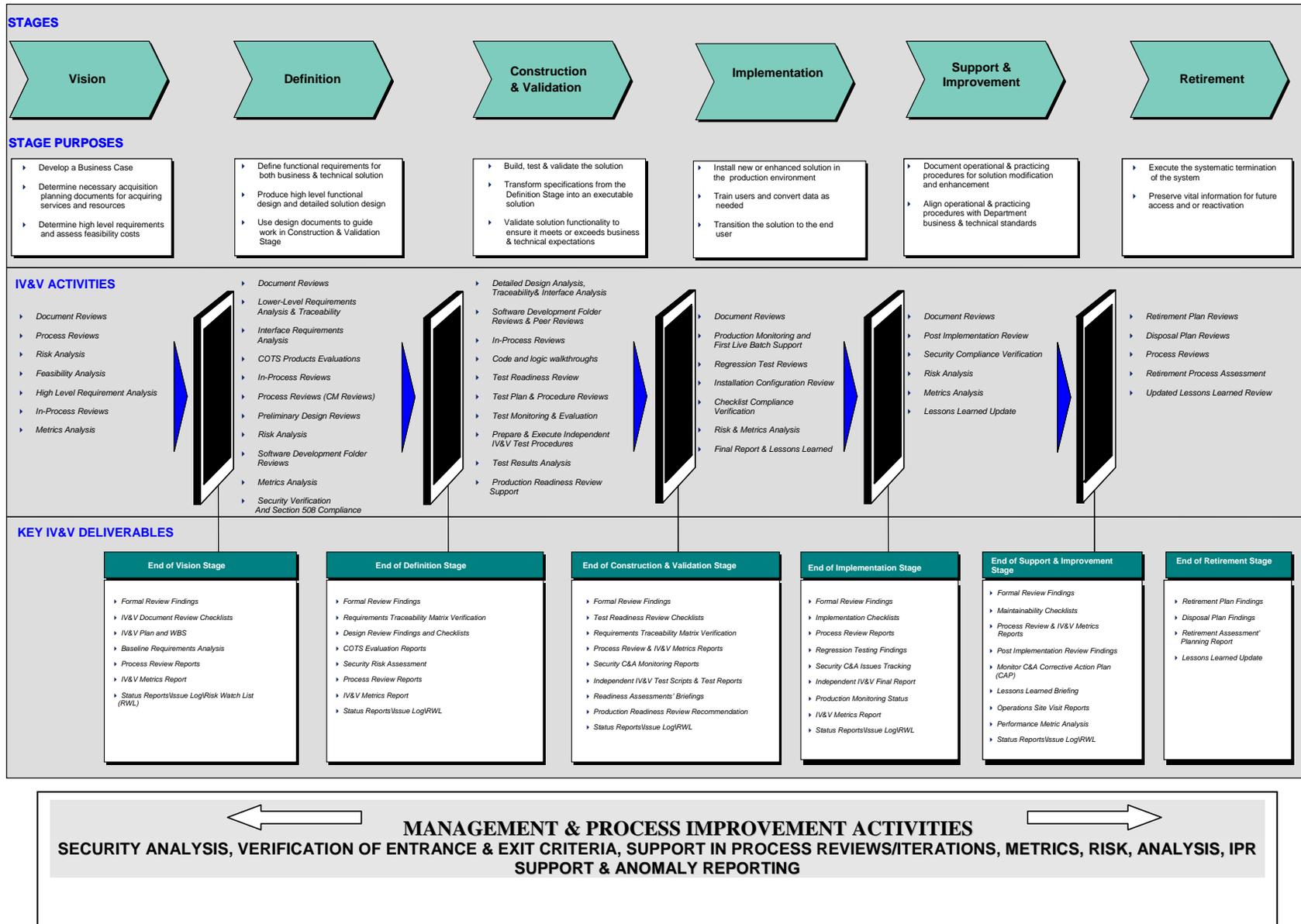
The U.S. Department of Education LCM Framework in combination with the Work Products Guide, provides an outline of a structured approach, providing required stages, key activities and core deliverables to provide a foundation for existing interrelated development and project

management processes used in delivering IT solutions. The IV&V Handbook will use the LCM Framework and Work Products Guide as the basis for its lifecycle methodology and will align the IV&V activities and core deliverables to these development stages. Through a stage gate review process, this Framework will focus on results obtained at the end of each stage to assist IV&V in assessing product quality, correctness and compliance to requirements and regulations. IV&V will work within this framework or any tailored lifecycle based on this framework, as long as the tailored process is approved by Federal Student Aid.

The Framework is comprised of six stages: 1) Vision; 2) Definition; 3) Construction and Validation; 4) Implementation; 5) Support and Improvement; and 6) Retirement.

Each stage consists of required key activities and core deliverables that must be completed prior to entry into the next stage. As previously stated, a detailed illustration of the Framework with accompanying IV&V activities is included in Exhibit 3-1. The Framework stages are designated by number followed by IV&V activities for each stage.

Exhibit 3- 1, Federal Student Aid IV&V Lifecycle Activities



3.3 LCM Vision Stage

The Vision Stage is the initial system lifecycle stage during which project scope, high-level requirements and user needs are documented and evaluated. During this stage, the IV&V team must have a clear understanding of the issues facing Federal Student Aid to ensure that the Statement of Work, Initiative Vision Document and Business Case correctly articulate the needs of Federal Student Aid. In this stage, the principal IV&V Team tasks will be evaluating the Business Case, acquisition documents, Project Concept Document, Project Charter, Performance Management, Government Quality Assurance Requirements and Communication Plans, Business Architecture Documents, security and privacy documents, and the tailored project guide. IV&V’s focus will be to determine whether the proposed solution satisfies user needs and project objectives, perform risk analysis, and analyze any limitations inherent in the recommended approach. The role of IV&V may be limited in this stage depending on the size of the project. The level of IV&V support would be at the discretion of Federal Student Aid based on recommendations from IV&V.

3.3.1 Vision Stage – Document Reviews

The IV&V Team will evaluate the Vision Stage documentation in terms of system performance needs, feasibility (e.g., overestimation of COTS capabilities), completeness, and accuracy. For system upgrades, the IV&V Team will analyze the impact of proposed target system changes on existing architecture and interfaces. The IV&V Team will assist in balancing performance improvements (e.g., new processors) with functional enhancements that require greater resources. Documents reviewed during this stage typically include the Business Case, Project Charter, Concept Documentation, Acquisition documents, Business Architecture documentation, security and privacy documents, tailored project guide, Government Project Management Plan, Statement of Objectives (SOOs), task order, initial Quality Assurance, Configuration Management, Requirements, Performance Management Communication and Transition Plans, feasibility studies, Work Breakdown Structure, high-level data flow diagrams, high-level business and functional requirements and rapid development or iteration plans.

Table 3- 1, Vision Stage - Document Reviews

Task	Description
Method:	<p>The IV&V Team will evaluate documents to ensure that they are complete, correct, consistent, specific, and unambiguous. Documents will be reviewed to ensure that they tailor and adhere to the Document Review Checklist, both in a “quick-look” as well as a full-up review. A coordinated comment package will be prepared, sent to Federal Student Aid, and an adjudication process initiated. During a typical document review effort, the IV&V Team will review multiple versions of all development documentation and submit comment packages for each. In order to resolve issues in a timely manner, critical issues or comments will be passed informally to the developer, and the IV&V team will work with the developer to resolve these issues in a timely fashion.</p> <p>The IV&V Team will apply static and dynamic analysis techniques in reviewing technical documentation. Static analysis techniques will be used to analyze the technical content and form of the documentation and to ensure the proper form for updated documents and</p>

Task	Description
	<p>programming products, such as source code. Dynamic analysis techniques will be used to assess the functional and computational correctness of the document and code. By using both techniques, the IV&V Team will perform a thorough analysis of the documentation, assuring correctness and testability of critical functional, security, and operational requirements.</p> <p>The following document review steps will be applicable to all subsequent document reviews referenced for other lifecycle stages, and will not be repeated in the following sections. The method used to evaluate the quality of the target system products will be comprised of six steps:</p> <p>STEP 1: Review the program product using the tailored Document Review Checklist, if applicable.</p> <p>STEP 2: Generate applicable comments.</p> <p>STEP 3: For critical reviews, IV&V may generate a “quicklook” preliminary technical report to Federal Student Aid. This report will include an assessment of the product's quality. This will not replace the more detailed review. An internal IV&V Team comment walkthrough will be performed for additional analysis and/or critique. All critical issues or comments will be communicated and adjudicated in a timely manner.</p> <p>STEP 4: Deliver the comment package to the Federal Student Aid client for review and, if approved, delivery to the developer.</p> <p>STEP 5: Upon receipt of the developer’s responses, evaluate the merit of those responses and meet to adjudicate any remaining issues. Send additional comments on responses, as necessary.</p> <p>STEP 6: At the conclusion of the review/adjudication process, re-evaluate the product quality based upon the status of the unresolved comment responses. If the product is considered to be of unacceptable quality, provide specific recommendations to Federal Student Aid for achieving acceptance. Verify that updates are incorporated in subsequent releases.</p>
Inputs:	Vision Stage Documentation
Outputs:	Findings
IV&V Standard Reference:	Section 2.5.3

3.3.2 Vision Stage – Risk Analysis

The IV&V Team will verify and validate proposed developer approaches for reducing developmental, technical, schedule, and cost risks. The IV&V Team will evaluate the developer’s proposed solution and processes. This evaluation will include verifying the adequacy of development technology and assumptions on the availability of Government Furnished Equipment (GFE) and/or COTS technologies. Appendix D provides a detailed process for performing risk analysis and also provides a template for the Risk Watch List.

Table 3- 2, Vision Stage - Risk Analysis

Task	Description
Method:	<p>Risk Management is a key component of IV&V and must be part of the full Lifecycle Framework. By using a risk-oriented approach, the IV&V Team will monitor the development effort and provide a targeted corrective action approach.</p> <p>The IV&V Team will maintain an independent Risk Watch List with recommend mitigation strategies. The Risk Watch List should be delivered to Federal Student Aid and the developer on a regular basis and the IV&V team should review all outstanding risks with Federal Student Aid and Development Program Managers. The more involved the program managers are in the process of risk assessment, the more likely all of the key risks will be identified. This should be reviewed against the Government Risk Lists as required by the Work Products Guide.</p> <p>The IV&V Team will conduct brainstorming risk analysis sessions to review potential risks. The IV&V Team will rank these risks and track them to mitigation. This independent risk analysis will help ensure that risks are identified and mitigated early in the process.</p> <p>The benefits of formalizing the risk management process will be:</p> <ul style="list-style-type: none"> • Identify issues that are actually project risks • Keep all identified risks easily visible at all times rather than just those risks that are high profile at any one time • Encourage the creation of strategies to keep risks from turning into problems • Track the risks to determine if the risk exposure changes with time • Track the risks to verify that they are addressed • Provide a framework for future improvement
Inputs:	Current Plans, Work Breakdown Structure (WBS), GFE and/or COTS Technologies Documentation, Business Case, Concept Documentation, Government Risk List, and the plans required for the Vision Stage.
Outputs:	Risk Watch List
IV&V Standard Reference:	Section 2.5.1

3.3.3 Vision Stage – In Process & Stage Gate Reviews

In Process & Stage Gate Reviews must be conducted during all lifecycle stages of development. The type of reviews may include a formal walkthrough of the tailored project guide, or Business Case. The Vision Stage provides a unique opportunity for identification of discrepancies when a change of course will have the least impact. The IV&V Team will support formal walkthroughs of documentation during this stage. Thorough, independent analyses will be performed and Vision Stage entrance and exit criteria verified at stage gate reviews to minimize any risk to the program. In addition, the IV&V Team will support all reviews as scheduled or required by the Project Charter.

Table 3- 3, Vision Stage - In Process & Stage Gate Reviews

Task	Description
Method:	<p>The IV&V Team will generate a tailored checklist for entrance/exit criteria verification verifying whether all items are satisfied. The IV&V Team will also verify that action items are documented and tracked. Vision Stage review criteria will include, as a minimum, the following:</p> <ul style="list-style-type: none"> • First Iteration of requirements and architecture documents, acquisition/contracts documents, technical documents, security and privacy documents and Business Case has been approved and agreed upon by stakeholder, including sponsors and advisors • Task Order reviewed, approved and awarded • Development of Project Charter • Preliminary WBS has been approved • High Level requirements developed and approved • Security Certification & Accreditation (C&A) Planning • Project Management Plan completed • IV&V Plan developed and approved
Inputs:	Entrance Criteria, Exit Criteria, Tailored Criteria Checklist
Outputs:	Completed Checklist, Findings, IV&V Plan
IV&V Standard Reference:	Sections 2.5.2, 2.5.10

3.3.4 Vision Stage – Process Reviews

Throughout the lifecycle, the IV&V Team will perform a review of the developer's processes, based on their documented plans, with particular emphasis during the early stages. Process reviews will be discussed exclusively in this stage to avoid redundancy. These assessments will be performed using multiple criteria including task orders, government and developer plans and required standards. The IV&V Team will also evaluate the developer's proposed use of commercial and custom software development/test tools. Some methodologies may include an iterative process that relies on the re-enactment of the "same" defined process over a number of iterations. This repetitive nature of process enactment, and the assessment of status metrics and lessons learned at each stage and iteration, provides an opportunity for fine-tuning the process for each successive iteration. As configuration management practices are key to a successful development effort, this process will be reviewed by the IV&V Team during the Vision and Definition Stages to ensure that an effective process is in place.

Table 3- 4, Vision Stage - Process Reviews

Task	Description
Method:	Process reviews will be scheduled through Federal Student Aid and coordinated with the

Task	Description
	<p>developer’s schedule and will be structured to minimize any impact to the development team. The IV&V Team will prepare a review plan that identifies the processes to be reviewed, dates, points of contact, review activities, and methods for performing the reviews. The process review will search for objective evidence that the developer is actually following established plans, and that all relevant practices are carried out. The process will be evaluated against the established plans and where appropriate, source documents will be traced through the process and the results will be evaluated. The review plan will be approved by Federal Student Aid in advance. Tailored checklists will be prepared as necessary based on the developer’s established plans. The process review will concentrate on the actual software development processes and artifacts that represent the target system at that point in its development.</p>
Inputs:	<p>Approved Review Plan, Process Review (CM) Checklist, appropriate process plans, (e.g., CM Plan, etc.).</p>
Outputs:	<p>Completed Checklist, Review Report</p>
IV&V Standard Reference:	<p>Section 2.5.9</p>

3.3.5 Vision Stage – Feasibility Analysis

A specification is feasible to the extent that the lifecycle benefits of the specified system meet or exceed its projected lifecycle costs. Feasibility analysis includes verifying that a system can be developed that satisfies the requirements within costs. The IV&V Team may perform cost benefit analysis at the option of Federal Student Aid, analyze schedules and review Vision documentation to assist Federal Student Aid in determining the feasibility of upgrades and enhancements. In addition, IV&V will assist Federal Student Aid with its Business Value Initiative planning.

Table 3- 5, Vision Stage - Feasibility Analysis

Task	Description
Method:	<p>The IV&V Team will review results of feasibility analyses or perform independent feasibility assessments of new developments and corresponding schedules. The IV&V Team will analyze the documentation and requirements against the proposed schedule. The IV&V Team will provide independent estimates of time for completion based on concept and high-level requirements. All options will be reviewed via team brainstorming sessions and alternative analysis and weighted. In addition, during rapid development projects where the data is available early, COCOMO analysis will be used where appropriate to validate the SLOC estimates. As a final activity, risk analysis will be performed to compare the risks of each option.</p>
Inputs:	<p>WBS, High-Level Business Requirements, Business Case, and High-Level System Flow if available, Business Architecture Documents, Initiative Vision Document, Project Concept Document, Required Vision Stage Plans</p>

Task	Description
Outputs:	Feasibility Assessment Report
IV&V Standard Reference:	Section 2.5.12

3.3.6 Vision Stage – High Level System Requirements Evaluation

Requirements traceability is a process of establishing that the needs of the users and target system are adequately stated in the documents comprising the governing set of requirements specifications. During this stage, Business Cases are developed and high-level requirements are defined in the form of the Requirements Development and Management (RDM) Document.

Table 3- 6, Vision Stage - High Level System Requirements Evaluation

Task	Description
Method:	The IV&V Team will review the requirements and initiate the generation of an independent RTM to verify requirements are in accordance with standards provided in Section 2. In addition, the SOW requirements will be evaluated as the basis for traceability activities and Baseline Requirements Analysis. The requirements will be gathered by the developer during requirement review sessions and provided at a high level in the form of a Business Case. In some cases, requirements may need to be derived by the IV&V Team or gathered from documentation, such as the RDM. In instances where IV&V starts late in the process or no requirements are available, Design Documentation may be used. The RTM will later be used to support the identification of requirements that do not trace to lower level documents, code, and test suites as they are delivered in each subsequent stage. The requirements will be evaluated for consistency and correctness and verified against any applicable IV&V results from the requirement derivation meetings. Any RTM must trace directly to the SOW, Business Case and Business Performance model through all stages of development.
Inputs:	Vision Stage Documentation, Developer’s Business Case, Statement of Work, Requirements Review Checklist
Outputs:	Completed Checklist, RTM, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.4

3.3.7 Vision Stage – Security Activities

The IV&V Team will review the results of all security reviews and will ensure Security requirements are included as part of the Business Case. The IV&V Team will work with the assigned System Security Officer and keep him/her abreast of any IV&V identified security issues.

Table 3- 7, Vision Stage - Security Activities

Task	Description
Method:	<p>At the end of the Vision Stage, the IV&V Team will ensure the security and privacy documentation, including the Critical Infrastructure Protection Questionnaire (CIP), has been completed and signed off by the Security Officer and includes the completion of all security related activities, including:</p> <ul style="list-style-type: none"> • Security Requirements as reflected in the Business Case • List of Business Partners Prepared and Approved • Generated Assignment Letters • Established Security Artifact File System
Inputs:	Business Case, RTM, Assignment Letters, Business Partner List, Requirements Matrices, Privacy Impact Assessment, Change Requests, Inventory Worksheets, Government Product Acceptance Plan, Project Management Plan
Outputs:	Findings
IV&V Standard Reference:	Sections 2.5.2, 2.5.10

3.3.8 Vision Stage – IV&V Metrics

The IV&V Team will internally track metrics during all stages of development and will report any concerns or issues via a Memorandum of Record (MOR), the Risk Watch List, Issue Log, Weekly Status Report, or IV&V Metrics Report, where applicable. The method of reporting is at the discretion of the IV&V Team, based on the scope of the effort, and/or the preference of the Federal Student Aid Task Manager. The key to success is selecting appropriate metrics, especially metrics that provide measures over the entire software lifecycle, and address both software processes and products. Section 6 provides a methodology for preparing, tracking and reporting IV&V metrics based on defects accumulated from product and process reviews.

Table 3- 8, Vision Stage - IV&V Metrics

Task	Description
Method:	<p>To ensure IV&V effectiveness, tracked metrics must be tailored and used, or gathering them can be a wasted exercise. In choosing metrics, several factors should be considered:</p> <ul style="list-style-type: none"> • The intended use of the metrics data • The usefulness and cost effectiveness of the metrics • The application’s engineering installation platform • Type of development, e.g., web, COTS, OOD <p>During this early stage, the metrics will focus on the WBS and the accuracy and correctness of the schedule. All deviations from the schedule will be tracked and significant slippage will be reported. Requirement changes will be tracked, monitored and verified. Metrics will vary from project to project, but in this early stage the emphasis will be on estimating techniques and the accuracy and consistency of the developer’s</p>

Task	Description
	planning activities.
Inputs:	Business Case, RTM, WBS, Government Project Management Plan
Outputs:	IV&V Metrics Report and inputs to regular status reporting and risk/issue logs.
IV&V Standard Reference:	Section 2.5.6

3.4 LCM Definition Stage

The Definition Stage is the period of time during which the Business Case Requirements are further defined into business, functional and security requirements that address both the business and technical solution. In addition the project team will develop a high-level functional design and detailed solution design to be used in the Construction and Validation Stage. In this stage, the IV&V Team will continue to monitor the development effort and will trace the requirements through the high-level and detailed design and monitor the further refinement of the RTM. As this stage proceeds, many of the functional and performance capabilities are further defined and documented in the developer RTM, Business Case and Performance Model which will be verified and baselined by the IV&V Team. During the Definition Stage, the IV&V Team will perform document reviews, requirements and COTS evaluations, and participate in preliminary design reviews, and In Process Reviews.

3.4.1 Definition Stage – Document Reviews

The IV&V Team’s focus on the requirements documentation will be to ensure that all of the requirements documents are reviewed as early in the LCM as possible. The IV&V Team will review the requirements documentation and the RTM to ensure that the requirements are adequately captured and baselined. During this stage, the IV&V Team will also review design and requirements documentation, system performance model criteria, the Project Management Plan, Configuration Management Plan, updated business cases and updated security and privacy documentation. The IV&V Team will review preliminary and detailed designs to ensure they fully address and are consistent with the development effort. IV&V will ensure each plan is a complete specification of the tasks required to achieve the objectives. In addition, all of the test plans will be reviewed to ensure that they present a sound and realistic approach to testing. The IV&V Team will document errors and omissions and report them to Federal Student Aid.

Table 3- 9, Definition Stage - Document Reviews

Task	Description
Method:	The IV&V Team will perform system and requirements specification and design analyses to ensure that the system level requirements are sufficiently identified to enable an allocation to hardware and software requirements. The IV&V Team will review the

Task	Description
	preliminary and detailed design and test-planning documents to ensure that standards and conventions from Section 2 are followed and that the items from the Design Review Checklists are on schedule.
Inputs:	RTM, Requirements Specifications, Preliminary and Detailed Design Documentation, Government and Contractor Project Plans, Test Planning Documentation, Master Test Plan, Data Management Plan, Software Architecture Documentation, Integrated Baseline Review Report Transition Plan, Checklists, IV&V RVM, Document Review Checklist
Outputs:	Findings, Completed Checklist
IV&V Standard Reference:	Section 2.5.3

3.4.2 Definition Stage – Requirements and Traceability Analysis

Requirements traceability is a process of establishing that the needs of the users and target system are adequately stated and comprise the governing set of requirements specifications. This body of documents can include the System Specification, Human Computer Interface (HCI) definitions, requirement specification documents and interface requirements documentation.

Table 3- 10, Definition Stage - Requirements and Traceability Analysis

Task	Description
Method:	This will be an iterative process performed at each stage and for each delivery of requirements documentation. The IV&V Team will review the requirements to ensure that the target system requirements are stated as binding (i.e., as shall) and are testable. For any requirement that is partially or completely stated in a referenced document, the requirement will be traced to that document and reviewed to ensure that all necessary information is specified therein. The IV&V Team will later trace these requirements to the Design and Test Documentation. If applicable, an independent developer RTM will also be compared to the developer RTM, and discrepancies will be resolved.
Inputs:	Requirements Specification, Developer's RVM, IV&V RTM, Requirements Review Checklist, Security requirement documents
Outputs:	Completed Checklist, RTM, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.4

3.4.3 Definition Stage – Interface Requirements Analysis

Interface requirements analysis is the process of ensuring all of the internal and external interfaces to the software are completely and correctly specified. The common implementation

of software reuse and standard COTS software components increase the importance of independent interface analysis by the IV&V Team.

Table 3- 11, Definition Stage - Interface Requirements Analysis

Task	Description
Method:	The IV&V Team will verify the protocols for transferring and receiving data across interfaces are in accordance with Section 2 standards, interface data are accurately described, and all of the interface documentation is consistent. In addition, the IV&V Team will compare each function’s input data and source to the associated output data and destination, and trace this data through the interface documents. IV&V will review the Intersystem Specification document and Inter-System Test Plan to ensure that all of the interfaces are addressed for the system under development.
Inputs:	Interface Documentation, Requirements Documentation, RTM, Functional Flows, Architecture documents, Requirements Review Checklist
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.4

3.4.4 Definition Stage – COTS Products Evaluations

The IV&V Team will independently evaluate COTS products at the request of Federal Student Aid.

Table 3- 12, Definition Stage - COTS Products Evaluations

Task	Description
Method:	The IV&V Team will evaluate COTS tools based on requirements and fitness for purpose. The latest industry periodicals, the Internet, and discussions with vendors will be the source of data for analysis and evaluation. In addition, the IV&V Team will talk to other agencies and organizations using the tool in a similar environment as Federal Student Aid for lessons learned and to uncover any potential problems. The IV&V Team will provide Federal Student Aid with recommendations and/or proposed alternatives.
Inputs:	Vendor Documentation, Reference Material, Other government Agency Lessons Learned
Outputs:	Findings
IV&V Standard Reference:	Section 2.5.3

3.4.5 Definition Stage – In Process & Stage Gate Reviews

The Definition stage still provides an early opportunity for identification of discrepancies when a change of course in the project will have less impact; and for this reason, stage gate reviews are

critical. The IV&V Team will support all System Requirements Reviews, Preliminary and Detailed Design Reviews, Test Plan Reviews and other formal reviews during this stage. Thorough, independent analysis will be performed and entrance and exit criteria verified to minimize risk to the program. The IV&V Team will continue to be a key participant in the Integrated Product Team.

Table 3- 13, Definition Stage - In Process & Stage Gate Reviews

Task	Description
Method:	<p>The IV&V Team will generate a tailored checklist for entrance/exit criteria verification and verify that all items are included. The IV&V Team will also verify that actions are documented and tracked. During this stage, the IV&V Team will support meetings and formal reviews such as In Process Reviews, and the Design Reviews. For the Preliminary and Detailed Design Reviews, the entrance criteria will be rigorously reviewed, while the Design Checklists provides information on types of items to be evaluated. This checklist will be tailored for the target system under development.</p> <p>Review Criteria as defined by the LCM will include, as a minimum, the following:</p> <ul style="list-style-type: none"> • All updates to the WBS, Business Case and Performance Model are approved • Project Management Approach • RTM has been baselined and traces to design • Preliminary and Detailed Design Approved • QA, Project Management (PM), CM and Test Plans have been reviewed and approved • Project risk and issues are manageable <p>The IV&V Team will utilize a design checklist for evaluating whether entrance/exit criteria have been met. The IV&V Team will verify that action items from all reviews are documented, tracked and resolved. Preliminary Design criteria include as a minimum: (1) Business process continues to support Value and Success measures identified in Vision Stage, and (2) All of the components necessary to support the business solution design have been identified and described in enough detail to assess system complexity to build it. Detailed Design Criteria will include, as a minimum, the following:</p> <ul style="list-style-type: none"> • Designed components cover complete scope of project solution • Detailed design thorough and complete • Sources of data for conversion identified and mapped • Screens, forms, and reports are user-friendly • IV&V report issues are satisfactorily resolved
Inputs:	Entrance Criteria, Exit Criteria, Software Architecture Document, Requirements Specification, Use Case Data, Tailored Criteria Checklist, Requirements Review Checklist, Preliminary Design Review (PDR) Checklist
Outputs:	Completed Checklists, Findings
IV&V Standard Reference:	Sections 2.5.2, 2.5.3, 2.5.9, 2.5.10

3.4.6 Definition Stage – Process Reviews

As CM practices are key to a successful development effort, this process will be reviewed for the second time to ensure an effective process remains in place and is compliant with the delivered plan in the stage. In addition, the IV&V Team will monitor all of the developer processes and look for areas to review and opportunities for improvement.

Table 3- 14, Definition Stage - Process Reviews

Task	Description
Method:	Process reviews will be scheduled through Federal Student Aid and coordinated with the developer's schedule and will be structured to minimize any impact to the development team. The IV&V Team will prepare a review plan that identifies the processes to be reviewed, dates, points of contact, review activities, and methods for performing the review. The process review will search for objective evidence that the developer is actually following established plans and that all relevant practices are carried out. The process will be evaluated against the established plans and where appropriate, source documents will be traced through the process and the results will be evaluated. The review plan will be approved by Federal Student Aid in advance. Checklists will be prepared based on the developer's established plans. The process review will concentrate on the actual software development processes and artifacts that represent the target system at that point in its development.
Inputs:	Approved Review Plan, CM Checklist, Process Review (CM) Checklist, Appropriate process plan, (e.g., CM Plan, etc.)
Outputs:	Completed Checklist, Review Report
IV&V Standard Reference:	Section 2.5.9

3.4.7 Definition Stage – Risk Analysis

The IV&V Team will continue to monitor project risks and will maintain the Risk Watch List. The Risk Watch List should be delivered to Federal Student Aid on a regular basis, and the IV&V team should review all outstanding risks with Federal Student Aid and Development Program Managers. The Risk Watch List will include a column for developer response to allow the developer an opportunity to provide their response to each risk.

Table 3- 15, Definition Stage - Risk Analysis

Task	Description
Method:	The IV&V Team will continue to maintain an independent risk watch and recommend mitigation strategies. The focus of the risk analysis will include documentation of requirements, level of traceability and adherence to schedule. IV&V will monitor external conflicts, dependencies and entities impacting the effort.

Task	Description
Inputs:	Current Plans, WBS, RTM, RDM, RVM, Business Case, preliminary design documentation, preliminary test and security plans, performance models, Government and Contractor Risks
Outputs:	Risk Watch List, findings
IV&V Standard Reference:	Section 2.5.1

3.4.8 Definition Stage – Design Evaluation and Traceability Analysis

A Design Review is the formal technical review of the basic design approach. During this stage, all development and test tools that are planned for use during program development will be identified. The IV&V Team will continue risk and schedule analysis, support design walkthroughs, and perform reviews of preliminary design documents. This can include updates to the risk assessment, a plan showing the number and contents of each iteration, draft test planning documentation, measurable evaluation criteria for assessing the results of the initial iterations, and a software architecture description (stating constraints and limitations). It is crucial that the IV&V Team perform a rigorous review of the exit criteria for the preliminary and detailed design reviews to ensure a successful design and minimize potential rework. The IV&V Team may also review the interface definitions, prototype efforts, and process infrastructure. As appropriate, the IV&V Team may provide alternatives to the proposed architecture for consideration by the community or may independently evaluate any proposed alternative design concepts and reconcile the results with those of the development contractor. The IV&V Team will review the target system design in preparation for the design reviews. The IV&V Team will review and evaluate the design documents, such as descriptions of the technical architecture, business process flows, HCI descriptions, and system screens.

Table 3- 16, Definition Stage - Design Evaluation and Traceability Analysis

Task	Description
Method:	<p>The IV&V Team will evaluate the developer's basic system architecture based on the Section 2 standards and the checklist items. Developer tools will also be reviewed as appropriate (e.g., Rational Suite), to assess the design activities. The IV&V Team will seek to prevent design errors from being implemented into the solution and provide assurance that the design is optimized. To support the detailed design, the IV&V Team will:</p> <ul style="list-style-type: none"> • Evaluate the evolving design and architecture • Evaluate the technical documentation • Verify that the developer RTM adheres to the design • Conduct a design traceability analysis • Review the results of peer reviews or JAD Meetings • Participate in design reviews and technical interchange meetings

Task	Description
	<p>Traceability will be performed between the software design documents and the software requirements documentation, based on Section 2 standards. The requirement trace will be performed in both directions between requirements and design. The trace analysis will be performed to ensure that no requirements are omitted or implemented more than once, no extraneous design requirements exist, and a requirement addressed by more than one design element is completely and consistently satisfied.</p> <p>The IV&V Team will verify the traceability among the engineering models (design models, source code, and executable components). As part of the design evaluation, the IV&V Team will evaluate the design documentation’s data flows and entity relationship diagrams, pseudo-code, sample screens and layouts, forms and reports, and internal and external interfaces.</p> <p>Design traceability analysis will ensure that all requirements have been allocated to the design documents and that the design documents contain only requirements that are detailed in the software requirements documents. The IV&V Team will examine each of the design documents and verify the developer has correctly and completely extracted the requirements for the item to be traced. The IV&V Team will resolve any conflicts among the document requirements in accordance with the order of precedence clause within the contract and/or by obtaining guidance from Federal Student Aid. When performing traceability, the IV&V Team will detect:</p> <ul style="list-style-type: none"> • Requirements in the subordinate documents that do not connect to any baseline requirement • Requirements that are in the baseline document, but are not connected to the subordinate document <p>When database conversions are required, the IV&V Team will observe the process to ensure that proper CM controls are being followed and may, if necessary, re-evaluate the schema for normalization based on the platform. The IV&V Team may also verify the data integrity, after the conversion is complete, through query testing and statistical sampling.</p> <p>HCI assessments will be performed to evaluate the user interface and its fitness for the user community.</p>
Inputs:	Design Documentation, Requirements Allocation Matrix, Requirements Database, Sample Screens and layouts, Forms and Reports, Requirements Review Checklist, Architecture Documents, Use Cases, Requirements Specification, Master Test Plan, Process Review CM Checklist, functional flows and entity relationship diagrams (ERD), data dictionary, pseudo-code, and internal and external interfaces. SDF and SDF Review Checklist, Requirements Documentation, Design Checklists
Outputs:	Completed Checklists, Findings
IV&V Standard Reference:	Sections 2.5.2, 2.5.3, 2.5.9, 2.5.10, 2.5.12

3.4.9 Definition Stage – Software Development Folder Reviews

As development materials are documented, the developers typically establish a file structure on either the Department of Education’s Federal Student Aid Network, also known as EDUCATE, or within their own tool suite depending on their contract with Federal Student Aid. Also, Federal Student Aid is standardizing on the Rational Suite, which would provide a consistent

method for capturing SDFs. One method to allow easy access to all development materials is for the developer to provide access to their SDFs. It is imperative that the IV&V Team gain access to this resource as soon as it is established and become familiar with the directory or file structure.

Table 3- 17, Definition Stage - Software Development Folder Reviews

Task	Description
Method:	<p>During the system lifecycle, the IV&V Team will monitor the development documentation and/or SDFs to ensure their currency and for compliance with Section 2 standards. The IV&V Team will perform a formal detailed review of the SDFs at the midpoint and conclusion of the Detailed System Design. The reviews of the SDFs will be coordinated with the developer and timed to minimize impact on the development effort. The IV&V Team will tailor the SDF Review Checklist and use this as the basis of the review.</p> <p>For the Definition Stage, the IV&V Team will review the SDFs and evaluate all of the preliminary planning documentation, design notes, algorithms, and updated requirements. Detailed design documentation will be reviewed along with any Program Design Language (PDL), web screens and source code. With an Object Oriented development effort, the IV&V Team will review the outputs of the developer's tools to support assessments of the design. The IV&V Team will continue to perform periodic reviews of the SDFs throughout the lifecycle, but it will only be included in this stage to avoid redundancy. The purpose of these reviews will be to verify that the source code is under CM control, the code is written in accordance with Federal Student Aid traditional and web-based coding standards, and the proper supporting documentation is present in the SDF. Supporting documentation includes design notes, allocated requirements, and unit test plans and results. In addition, peer review details, action items and any anomaly documentation should also be present within the documentation.</p>
Inputs:	Design Documentation, Development Documentation, SDF Artifacts, RTM, SDF Review Checklist
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.4, 2.5.8, 2.5.9

3.4.10 Definition Stage – Security Activities

The IV&V Team will assess the results of all security reviews and will ensure that Security requirements are traced through the Business Case, RDM and design. The IV&V Team will continue to work with the assigned System Security Officer (SSO) and keep him/her abreast of any IV&V security issues. In addition, IV&V will support the initial planning for the C&A Process.

Table 3- 18, Definition Stage - Security Activities

Task	Description
Method:	<p>At the end of the Definition Stage the IV&V Team will ensure that the Security requirements have been completed, fulfilled and signed off by the Security Officer and includes the completion of all security related activities including:</p> <ul style="list-style-type: none"> • System Roles and Responsibilities Defined • System Identified in terms of type (new or upgrade) and level of sensitivity • Completed Threat and Vulnerability Assessment • Security Guidance Compliance Matrix • Completed Interconnected System’s Security Documentation • Completed Drafts of Memoranda of Understanding and Service Level Agreements • C&A Project Plan (C&A Plan) • System Rules of Behavior documented • Approved Contractor Access Request Form
Inputs:	<p>Business Case, RTM, Assignment Letters, Business Partner List, Requirements Matrices, security requirements, security documentation including Security Plan, Disaster Recovery Plan, Continuity of Support Plan, and Risk Assessment Plan and Mitigation Plan, Information Technology Contingency Plan, Government and Contractor Security Risks, Master Test Plan</p>
Outputs:	<p>Findings</p>
IV&V Standard Reference:	<p>Sections 2.5.2, 2.5.10</p>

3.4.11 Definition Stage – Section 508 Compliance Review

This initial Section 508 Review determines the degree of compliance with Section 508 of the Rehabilitation Act and associated amendments of 1998. The purpose of this review is to ensure that the development team is coordinating with the appropriate contacts at the Department of Education with regard to Section 508, and that HCI requirements are in place for Section 508 compliance.

Table 3- 19, Definition Stage - Section 508 Compliance Review

Task	Description
Method:	<p>The IV&V Team will evaluate the developer’s approach to Section 508 compliance and determine if the requirements have been addressed and if the development team is coordinating with the Department of Education’s internal Section 508 point of contact. This is not meant to be a review of the application for compliance, as this is performed internally by the Department of Education. However, if requested by Federal Student Aid, the IV&V agent can participate in the assessment. Section 508 compliance would address:</p>

Task	Description
	<ul style="list-style-type: none"> The main processing sites The links interconnecting these sites These sites' connections to the auxiliary sites as well as to the VDC
Inputs:	Section 508 Checklist, Reference Material, RTM
Outputs:	Part of Risk Watch List or MOR
IV&V Standard Reference:	Sections 2.5.2, 2.5.3, 2.5.8

3.4.12 Definition Stage – IV&V Metrics

The IV&V Team will continue to track metrics during this stage of development and will report any concerns or issues via the IV&V Metrics Report and as part of the Risk Watch List, Issue Log or Weekly Status Report.

Table 3- 20, Definition Stage - IV&V Metrics

Task	Description
Method:	During this stage, the metrics will focus on the Requirements, Design and the accuracy of the schedule. All deviations from the schedule will be tracked, and significant slippage will be reported. Requirement changes will be tracked, monitored, and verified.
Inputs:	Business Case, RTM, WBS
Outputs:	IV&V Metrics Report or inputs to regular status reporting and risk/issue logs
IV&V Standard Reference:	Section 2.5.6

3.5 LCM Construction and Validation Stage

The objective of the LCM Construction and Validation Stage is to build, test and validate the solution, transform specifications developed in the previous stage into an executable solution and validate solution functionality to ensure it meets or exceeds business and technical expectations.

3.5.1 Construction and Validation Stage – Document Reviews

The IV&V Team will review the updates to the previous stage documentation in addition to the core documents for this stage to include: Testing Documentation, Implementation Documentation and Operations and Maintenance documentation. In addition, this stage includes a review of the updated test plans and detailed test procedures. During this stage the source code

and accompanying documentation may also be reviewed at a high level to ensure that Federal Student Aid coding standards, provided in the LCM documentation, are being followed.

Table 3- 21, Construction and Validation Stage - Document Reviews

Task	Description
Method:	The IV&V Team will apply a complete and thorough trace of the requirements to the test scripts. The IV&V Team will review test documentation to ensure that standards and convention from Section 2 are followed. The updated test scripts, results and reports will be reviewed. All of the implementation documentation will be reviewed including the Implementation Plan, security documentation, Training Plan, User Manuals, Data Conversion and Migration Plans and Operations and Maintenance Plans. All of the Production Readiness Review Documentation will be reviewed. The Document Review Checklist will be used to ensure consistency in the reviews and will be tailored based on the review performed.
Inputs:	Test Plans, Suites, and scripts, RTM, Draft Conversion, Migration and Implementation Plans, Test Data, Test Descriptions and Procedures, SDFs, Solution User Manual, Document Review Checklist, C&A Standards, Implementation Plan, Plan of Action and Milestone Review, Completed TRR Checklist
Outputs:	Findings, Completed Checklists,
IV&V Standard Reference:	Section 2.5.3

3.5.2 Construction and Validation Stage – Performance Model Evaluation

The IV&V Team may validate the developer's performance model, if applicable, and assess model reliability. This validation effort will be conducted at the level of detail necessary to evaluate processor utilization, communications, capacity, storage requirements, and peak performance.

Table 3- 22, Construction and Validation Stage - Performance Model Evaluation

Task	Description
Method:	The IV&V Team may confirm that baseline products used by the modeling team are consistent with the controlled baseline documents. Wherever possible, the IV&V Team will validate the model using actual benchmark data. The IV&V Team will meet with the modeling team to discuss technical data relative to the model.
Inputs:	Baseline Documentation List, Benchmark Data (if available), Interviews
Outputs:	Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.7, 2.5.12

3.5.3 Construction and Validation Stage – Peer Reviews

The IV&V Team will review the records of the developer's peer reviews and design and code walkthroughs on a periodic basis, assuring that all pre-meeting, meeting, and post-meeting walkthrough requirements and tasks have been completed. Specifically, the IV&V Team will examine the following items: relevant documentation for the item under review, current system software standards and practices manual, minutes from the previous peer review, and evidence of action items being tracked to closure.

Table 3- 23, Construction and Validation Stage - Peer Reviews

Task	Description
Method:	The IV&V Team will assess the degree to which design requirements are being fulfilled during the peer reviews. The IV&V Team will also determine whether questions or problems resulting from the reviews are recorded as action items and assigned due dates for resolution. As a part of this process, the IV&V Team will submit its findings to assist the developer.
Inputs:	Meeting Minutes, Action Item List, Process Review CM Checklist
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.5.9, 2.5.10, 2.5.11

3.5.4 Construction and Validation Stage – In Process & Stage Gate Reviews

The IV&V Team will support meetings and formal reviews such as IPR and formal Stage Gate Reviews. For the major milestone reviews, IV&V will analyze both entrance and exit criteria.

Table 3- 24, Construction and Validation Stage - In Process & Stage Gate Reviews

Task	Description
Method:	<p>The IV&V Team will tailor and utilize the Checklists for entrance/exit criteria and to verify applicable items for the stage gate reviews. The IV&V Team will also verify all action items are documented, tracked, and resolved.</p> <p>Prior to the completion of the Construction and Validation Stage, the following exit criteria will be verified by IV&V:</p> <ul style="list-style-type: none"> • Design Documentation has been developed and approved • RTM is updated • A developed and tested solution has been completed and approved • Test Plans, Suites and Scripts have been developed and executed with verifiable test results • C&A Standards have been met

Task	Description
	<ul style="list-style-type: none"> • PRR has been conducted and signed off • Support Organization has been identified • Implementation Plan • Operations and Maintenance Plan • All IV&V reviews have been conducted satisfactorily
Inputs:	Entrance Criteria, Exit Criteria, Tailored Criteria Checklist, Critical Design Review (CDR) Checklist
Outputs:	Completed Checklists, Findings
IV&V Standard Reference:	Sections 2.3.2, 2.3.3, 2.3.9, 2.3.10

3.5.5 Construction and Validation Stage – Build Solution Source Code Traceability and Evaluation

During this stage, the IV&V Team will, at the option of Federal Student Aid, review the code in the SDFs. The IV&V Team will analyze a sample of the source code for traceability to the design document and conformance to developer and Federal Student Aid standards. The IV&V Team will also analyze the developer’s software metrics, if applicable.

Table 3- 25, Construction and Validation Stage - Build Solution Source Code Traceability and Evaluation

Task	Description
Method:	<p>The IV&V Team will review any changes to the software and selected portions of the source code in regard to traceability, ensuring the design requirements are met, and additional and/or unexpected requirements have been met. The level of sampling will be based on schedule, scope of the IV&V effort, and number of problems found during IV&V analysis. A requirements matrix will be used and discrepancies documented via an anomaly report. The developer will be notified immediately of discrepancies found within the developer’s requirements matrix.</p> <p>The IV&V Team will perform code inspections during the code and unit testing to identify problems early. The IV&V Team will perform detailed reviews on a portion of the source code. This sampling will be based on complexity and criticality. To verify maintainability, the IV&V Team will review the included source code comments to ensure sufficient support of the maintenance process and a review trail of the design. To verify consistency, the IV&V Team will review the source code standards and conventions established by the developer and approved by Federal Student Aid. When attending formal code reviews and inspecting code, the IV&V Team will use a customized checklist to evaluate the source code.</p>
Inputs:	The Enterprise IT Management’s Federal Student Aid Software Coding Standards. Source Code, Use Cases, Design Documentation, SDFs, Requirements, Code Review

Task	Description
	Checklist
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.6, 2.5.12

3.5.6 Construction and Validation Stage – Build Solution Unit Code and Logic Walkthroughs

The IV&V Team will periodically attend the developer's peer reviews and code walkthroughs to observe the review process, provide comments, and assure all pre-meeting, meeting and post-meeting walkthrough requirements and tasks are completed. Prior to the code walkthrough, the IV&V Team may review:

- The source code
- The unit test documentation
- The standards and conventions
- The unit design review minutes
- Any unit design waivers or deviations
- The developer's walkthrough checklist (if applicable)

IV&V will ensure code walkthroughs address all requirements of the design. During the walkthroughs, the IV&V Team will verify that questions or problems resulting from the walkthrough are recorded as action items with appropriate due dates for their resolution. IV&V will ensure that additional code walkthroughs will be scheduled following resolution of any particular applicable issues.

Table 3- 26, Construction and Validation Stage - Build Solution Unit Code and Logic Walkthroughs

Task	Description
Method:	The IV&V Team will periodically attend code and logic walkthroughs on selected code. The IV&V Team will verify that formal code inspections are performed by the developer for delivered software according to established plans.
Inputs:	Source Code, Meeting Minutes, Action Item List, Code Review Checklist, Process Review CM Checklist
Outputs:	Completed Checklists, Findings
IV&V Standard	Sections 2.5.3, 2.5.12

Task	Description
Reference:	

Optional tasks to be performed by the IV&V Team (as directed by Federal Student Aid) include:

- Conduct source code traceability and evaluation
- Perform source code and logic walkthroughs

This stage is concerned with system software development (i.e., coding and debugging) and unit testing. The IV&V Team will review the following artifacts: SDFs, code, technical and user documentation, unit test procedures, draft migration strategy, and the Implementation plan. The IV&V Team will review document updates as necessary, as well as the results of unit testing. The IV&V Team will review the draft test documentation as well to verify completeness and correctness. During this stage, the IV&V Team will assess the quality of developed program products including source code listings, draft user documentation, and draft software test procedures and descriptions.

3.5.7 Construction and Validation Stage – Build Solution Unit Test Analysis

The IV&V Team will perform assessments of unit testing. This includes reviewing the results of unit testing and verifying that unit testing was accomplished and all defects were documented and corrected.

Table 3- 27, Construction and Validation Stage - Build Solution Unit Test Analysis

Task	Description
Method:	The IV&V Team will verify that unit testing was performed and the information relating to the unit tests is adequately tracked in the appropriate test notebooks or SDFs. The criteria used by the IV&V Team to assess unit testing are included in the Testing Review/Review Checklist. This checklist should be tailored for each development effort.
Inputs:	Unit Test Plans, Suites and Scripts, Unit Test Results, Testing Review/Review Checklist, Federal Information Security Management Act of 2002 (FISMA) review findings.
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.4

3.5.8 Construction and Validation Stage – Test Readiness Review Support

The IV&V Team will encourage and support all Test Readiness Reviews (TRRs). This support includes verification of entrance and exit criteria to ensure readiness for testing. A sample TRR checklist is included in the appendix, and this can be tailored for each development effort. The

Enterprise Testing Standards Handbook provides the standards for Test Readiness Reviews. The following information is for IV&V analysis and evaluation of TRRs.

Table 3- 28, Construction and Validation Stage - Test Readiness Review Support

Task	Description
Method:	<p>Prior to the start of each test, the IV&V Team will support TRRs. Before beginning each TRR, the IV&V Team will verify that all of the entrance criteria have been satisfied. In addition, the IV&V Team will review all test suite documentation. Upon completion of the TRR, the IV&V Program Manager will provide a recommendation as to whether or not to proceed with testing. The TRR Checklist includes the types of items that are typically part of the entrance criteria for a TRR. This can be tailored to match the particular Federal Student Aid target system. TRR Criteria should include, as a minimum, the following:</p> <ul style="list-style-type: none"> • The scope, specific assumptions, and considerations for each level of application integration testing are clearly defined • The test environment(s) model the production environments as closely as possible, including production-sized databases, production LAN configurations, office setup, and all automated and manual processes • Detailed Integration Test Plan exists • Severity and volume of open problems acceptable to proceed • Interfacing systems prepared to participate in integration test or acceptable work-around in place • IV&V report issues satisfactorily resolved
Inputs:	Test Documentation, Requirements, Entrance Criteria, Exit Criteria, Tailored Criteria Checklist, TRR Checklist, FISMA Review Findings
Outputs:	Completed Checklists, Recommendations Relative to Start of Testing
IV&V Standard Reference:	Sections 2.5.2, 2.5.10

3.5.9 Construction and Validation Stage – Physical Test Environment Review

The physical test environment consists of the hardware, software, instrumentation, tools, simulators, and other support software necessary for testing the system. As part of IV&V test readiness evaluation, the physical test environment should be assessed to ensure that proper controls are in place and equipment and software are ready for test.

Table 3- 29, Construction and Validation Stage - Physical Test Environment Review

Task	Description
Method:	The IV&V Team will evaluate the test environment to verify that the proper controls are in place. Verification of the test environment will include witnessing the build, verifying that a clean install was accomplished, running a daily checksum and reviewing the output for accuracy, and checking that there are unbroken seals on the equipment. In addition, the IV&V Team will verify that proper CM controls are in effect, including control of test data and final procedures.
Inputs:	Test Documentation, Control Procedures, Process Review CM Checklist
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.4, 2.5.8

3.5.10 Construction and Validation Stage – Test Evaluation

During the test evaluation effort, the IV&V Team will independently assess the test program. Once the solution is developed, it is the responsibility of the Integrated Product Team to test the application to ensure that the test processes and products correctly and adequately demonstrate that the proposed solution meets the defined and approved functional, technical, and quality requirements. The IV&V test evaluation process begins with a review of the developer unit testing through review of the Integration, Performance, System and User Acceptance Test plans, execution, and results.

The developer will verify requirements at each level of testing with the expectation of observing "increasing levels of confidence" during each subsequent test. During the Acceptance Test, the IV&V Team may perform independent testing on the software. Final results of IV&V test findings will be compared to the appropriate developer test report and any discrepancies will be documented. To support Federal Student Aid during the formal testing, the IV&V Team will:

- Evaluate updated test plans and procedures
- Verify the integrity of the test environment
- Monitor execution of a sampling of test procedures
- Evaluate test results

Table 3- 30, Construction and Validation Stage - Test Evaluation

Task	Description
Method:	Evaluation of testing will be performed as testing progresses throughout this stage. The following tests are performed and are based on the LCM and Enterprise Testing Standards Handbook and may be tailored by Federal Student Aid. In Unit Testing , the tester examines each product component to verify that it works

Task	Description
	<p>independently. The IV&V Team is less involved in this phase but will verify that unit testing was performed and the information relating to the unit tests is adequately tracked in the appropriate test notebooks or SDFs.</p> <p>The Integration Test is the period of time in the lifecycle during which product components are integrated and the product is evaluated to determine whether target system requirements have been satisfied. The focus of this test is on how multiple components work together and the functions of the system. It will also test the user screens and system interfaces.</p> <p>The System Test is the period of time in the lifecycle during which the product is evaluated to determine whether functional and performance requirements have been satisfied. Performance Testing and Inter-System Testing are part of the System Test.</p> <ul style="list-style-type: none"> • Performance Testing is meant to simulate large transaction volume and test critical response times to evaluate the performance of the system during peak transaction periods. • Inter-System Testing verifies that the system functions with the interface required for the system. The file formats must be included and it is recommended that the files actually be exchanged between the systems in lieu of a visual approval of the file format. <p>User Acceptance Testing tests the requirements from a user perspective. They must include a robust set of test conditions to exercise the system in order to ensure that it meets predefined acceptance criteria.</p> <p>Post Implementation Verification is the final phase of testing that occurs after the application is deployed into production. IV&V monitors defects during this period, and when defects are critical or numerous, root cause analysis is recommended to determine why the defects occurred after User Acceptance Testing and identify process improvements to address any issues uncovered.</p> <p>IV&V Testing is performed by the IV&V Team to test procedures that were high defect, complex, or critical aspects of the system. It is a targeted approach that can be performed between System Testing and Alpha and Beta testing based upon system availability and Federal Student Aid discretion.</p> <p>The IV&V Team will support all levels of formal testing. All IV&V test team participants will be thoroughly conversant with the test organization and procedures. At the conclusion of each successful TRR, the IV&V Team will ensure that test bed configurations are identified, documented, and under developer configuration control, and that CM procedures are followed for control of the entire test environment including procedures, data, test bed, and software. The IV&V Team will evaluate developer test preparation to ensure that the developer has prepared detailed test plans and test procedures, has verified and revised these documents based on dry run results, and that requirements fully trace to test procedures.</p> <p>For each test, the IV&V Team will monitor test activities and procedure execution, evaluate the results, and assess proposed corrective actions.</p> <p>The IV&V Team will document any deficiencies and omissions discovered during each test evaluation. The IV&V Team will concentrate on weaknesses discovered in the developer's internal test to ensure the adequate exercise of those functions requiring more rigorous testing.</p> <p>To evaluate for completeness, the IV&V Team will monitor testing to determine the extent to which requirements are tested (i.e., stressed or exercised). If a functional requirement is tested, but not stressed, the requirement will be flagged as being exercised. For requirements claimed to have been previously tested, the IV&V Team will request</p>

Task	Description
	<p>and evaluate the associated test results.</p> <p>In its review, the IV&V Team may document, on a requirement-by-requirement basis, the extent to which each requirement was tested by the developer, and whether or not it was adequately tested. This assessment will help form the foundation of the IV&V Team’s assessment and targeted independent testing. For those tests that use an automated testing system, the IV&V Team will verify system adherence to the automated script used to execute and record the sequence test results.</p> <p>The IV&V Team witnesses will verify that the documented test plans and procedures are executed properly and that the designated requirements are adequately tested. The witnesses will immediately document test anomalies and/or departures from the approved detailed test procedures to provide reference points for later test evaluation and validation. For all anomalies, tests may be re-run by the developer using the same test procedures in an attempt to replicate the anomaly. Should additional test suites or slightly modified tests be required to determine an anomaly’s cause, the IV&V Team will ensure that these tests and modifications are thoroughly documented. Throughout testing, the IV&V Team will review all corrective actions and ensure that all change control procedures are implemented.</p>
Inputs:	Test Plans, Suites, and Scripts, Test Procedures, Use Cases, Test Results, Artifacts, CM Documentation, RTM, Security documentation
Outputs:	Findings, anomaly reports, MORs
IV&V Standard Reference:	Sections 2.5.1, 2.5.3, 2.5.4, 2.5.6, 2.5.9, 2.5.12

3.5.11 Construction and Validation Stage – IV&V Test Procedure Development

During this stage, the IV&V Team will continue the preparation of the procedures and use cases for the independent test procedures.

Table 3- 31, Construction and Validation Stage - IV&V Test Procedure Development

Task	Description
Method:	<p>The IV&V Team may prepare independent test procedures and use cases.</p> <p>The preparation of procedures and use cases will be an iterative process that continues throughout the test process. Following the monitoring of Developer Testing, the IV&V Team will revise the IV&V test procedures to incorporate more robust system testing for those areas of developer testing assessed as being less than adequate. Step-by-step procedures will be prepared together with expected results.</p>
Inputs:	Developer Test Procedures and Use Cases, RTM
Outputs:	IV&V Test Procedures and Use Cases

Task	Description
IV&V Standard Reference:	Section 2.5.5

3.5.12 Construction and Validation Stage – Test Reporting and Results Analysis

The IV&V Team will review test results to ensure that all relevant data has been captured and verified. This analysis will include a review of applicable test data and the test results generated by the developer. Upon testing completion, the developer will submit test reports detailing the developer's software testing results. The IV&V Team will review these test reports and forward any discrepancies to Federal Student Aid. In addition, the IV&V Team will prepare an independent test report documenting findings and lessons learned from the IV&V test activities.

Table 3- 32, Construction and Validation Stage - Test Reporting and Results Analysis

Task	Description
Method:	<p>The IV&V Team will confirm that all the requirements were properly satisfied, and all test procedure annotations and problems have been correctly documented. Through test observation and an off-line analysis of extracted test data, the IV&V Team will verify each formal test conducted by the developer. Following observation of the developer's tests, the IV&V Team will review the test execution reports and final test results to ensure that established test plan objectives were realized, test results were evaluated using the acceptance criteria defined in the approved test plan, and all test data conclusions are accurate and justified. In addition, the IV&V Team will analyze all tests containing deviations from the expected test results to ensure any problems associated with the deviations are documented for resolution and implementation. The IV&V Team will review the developer test reports to ensure that they adequately reflect the results of formal testing.</p> <p>Upon completion of the entire test activity, the IV&V Team will prepare an IV&V Test Report. The report will contain all of the IV&V Team's recommendations that were provided during the Acceptance TRR, IV&V test results and an assessment of the product's readiness for Implementation.</p>
Inputs:	Test Plan, Test Procedures, Use Cases, Test Results, Anomaly Reports
Outputs:	Additional Anomaly Reports, Findings, Completed Checklist, IV&V Test Report, Developer Test Report, Document Review Checklist, Test Results
IV&V Standard Reference:	Sections 2.3.3, 2.3.4

3.5.13 Construction and Validation Stage – Risk Analysis

The IV&V Team will continue to monitor project risks and will maintain a risk watch list. The risk watch list should be delivered to Federal Student Aid on a regular basis, and the IV&V

Team will review all outstanding risks with Federal Student Aid and Development Program Managers. The focus of the risk analysis will be the requirements, development and test. The ability to meet schedule and performance requirements will be evaluated by IV&V. In addition, the progress of testing and security will be reviewed.

Table 3- 33, Construction and Validation Stage - Risk Analysis

Task	Description
Method:	The IV&V Team will continue to maintain an independent risk watch list and recommend mitigation strategies. Requirements traceability, adherence to cost and schedule, level of user involvement, performance, and security are all issues reviewed during this level of risk analysis.
Inputs:	Design Documentation, WBS, RVM, RTM, Test Documentation, performance model, security documentation, Security Risk Assessment and Mitigation Plan, test artifacts, review results, Information Technology Contingency Plan
Outputs:	Risk Watch List, findings
IV&V Standard Reference:	Section 2.5.1

3.5.14 Construction and Validation Stage – IV&V Metrics

The IV&V Team will continue to track metrics during this Stage of development and will report any concerns or issues via an IV&V Metrics Report or as part of the Risk Watch List, Issues Log or Weekly Status Report.

Table 3- 34, Construction and Validation Stage - IV&V Metrics

Task	Description
Method:	<p>During this Stage, the metrics will focus on development and testing progress. Development metrics include changes to requirements. Any requirement changes will be tracked and monitored. All deviations from the schedule will be tracked, and significant slippage will be reported. Source code evaluation (total source lines of code or comparable measure of development estimation) will be used in a “planned” versus “actual” analysis.</p> <p>Test progress metrics will include a review of defects with trend analysis to assess time to correct the defects. The test status of requirements and number of test suites completed will be tracked throughout testing. Requirement test status will be monitored by disposition, (e.g., satisfied, failed, not tested, etc.).</p>
Inputs:	Business Case, RTM, source code, web pages, applets, WBS
Outputs:	Metrics, MOR, or inputs to regular status reporting and risk/issue logs
IV&V Standard	Section 2.5.6

Task	Description
Reference:	

3.5.15 Construction and Validation Stage – Security Activities

The IV&V Team must review the results of all security reviews and security testing and will ensure that Security requirements are traced through the Business Case, RTM and detailed test procedures. Security related plans that will be reviewed are the Security Plan, Disaster Recovery Plan and Continuity of Operations Plan. The IV&V Team will continue to work with the assigned SSO and keep him/her abreast of any IV&V security issues. C&A activities will be supported as detailed in Section 4 of this IV&V Handbook.

Table 3- 35, Construction and Validation Stage - Security Activities

Task	Description
Method:	<p>At the end of the Construction Stage, the IV&V Team will ensure that the Security deliverables have been completed and signed off by the SSO and includes the completion of all security related activities including:</p> <ul style="list-style-type: none"> • Draft System Security Plan • Draft Continuity of Operations Plan • Information Technology Contingency Plan • Security Risk Assessment and Mitigation Plan • Draft Disaster Recovery Plan • Draft C&A documentation • C&A Reviews • Risk Assessment • C&A Package • Configuration Management Plan • Privacy Impact Assessment • Threat Analysis • Impact Analysis • Risk Assessment Corrective Action Plan • Final Memorandum of Understanding (MOUs) and Service Level Agreements (SLAs) • Completed User Background Investigation Clearance Form • Approved User Access Request Form • System Access Letter to Contractor employees
Inputs:	RTM, Operation Procedures, Test Results, FISMA Review Findings
Outputs:	Findings

Task	Description
IV&V Standard Reference:	Sections 2.5.2, 2.5.10

3.5.16 Construction and Validation Stage – Section 508 Checklist Compliance Verification

The Section 508 Review is conducted to determine the degree of compliance with Section 508 of the Rehabilitation Act and associated amendments of 1998. The purpose of this follow-up review is to again verify that the test team is properly testing the Section 508 requirements and that any issues are highlighted prior to PRR.

Table 3- 36, Construction and Validation Stage - Section 508 Checklist Compliance Verification

Task	Description
Method:	The IV&V Team will evaluate the developer’s approach to Section 508 compliance and determine if the requirements have been addressed and if the development team is coordinating with the Department of Education’s internal Section 508 point of contact. This is not meant to be a review of the application for compliance, as this is performed internally by the Department of Education.
Inputs:	Section 508 Checklist, Reference Material
Outputs:	Part of Risk Watch List or MOR
IV&V Standard Reference:	Sections 2.5.2, 2.5.3, 2.5.8

3.5.17 Construction and Validation Stage – Readiness Reviews and PRR Support

It is recommended that Federal Student Aid have several readiness assessments during test activities and close to the PRR. This recommendation provides an opportunity to address any issues early in the process prior to PRR. The IV&V Team will support the readiness reviews and verify the entrance and exit criteria. At the discretion of Federal Student Aid, the IV&V Team will support a Functional Configuration Review and/or Physical Configuration Review. A Functional Configuration Review is the formal examination of a hardware/software configuration item's functional characteristics (prior to acceptance) to verify that the item has achieved the performance specified in applicable functional and allocated requirements. The Government Physical Configuration Review is the formal examination of a hardware/software configuration item's physical characteristics used to establish the product or operational baseline. In addition, it provides an accounting of all aspects of the software delivery to Federal Student Aid. IV&V will play a major role in the PRR and will provide a recommendation as to whether

the target system is ready for Implementation at least one day prior to the PRR date. In addition, the IV&V Project Manager will formally sign the recommendation.

Table 3- 37, Construction and Validation Stage - Readiness Reviews and PRR Support

Task	Description
Method:	<p>The IV&V Team will provide a recommendation as to whether the system is ready for operations at the readiness review. The IV&V Team will generate a checklist for entrance/exit criteria verification and will verify that all items are satisfied. The IV&V Team will also verify that action items are documented and tracked. In addition, the IV&V Team will review updated documentation prior to PRR. PRR Criteria will include, as a minimum, the following:</p> <ul style="list-style-type: none"> • Project value and success measures reasonably expected to be met or exceeded • Implementation procedures and programs successfully tested • Accuracy and completeness of converted data • Severity and volume of open problems acceptable to proceed • IV&V report issues satisfactorily resolved
Inputs:	<p>PRR Checklists, Test Results, IV&V Findings, Software and Hardware Inventory, Entrance Criteria, Exit Criteria, Tailored Criteria Checklist</p>
Outputs:	<p>Completed Checklists, Findings, PRR Recommendation, Executive Sign-off Sheet</p>
IV&V Standard Reference:	<p>Sections 2.5.2, 2.5.3, 2.5.4</p>

3.6 LCM Implementation Stage

The purpose of the Implementation Stage is to install the new or enhanced solution in the production environment, train users, convert data as needed and transition the solution to end-users. This is the stage where the hardware and/or software product goes into production and, if appropriate, is evaluated at the installation site to ensure that the product performs as required. Many operational support issues are under the domain of the VDC, and VDC procedures. The IV&V Team will support documentation reviews and the Operational Readiness Review (ORR) as well as review maintainability of the system. To support Federal Student Aid during the Implementation Stage, the IV&V Team will:

- Evaluate Implementation Stage documents
- Support the Transition to Production Conference Calls
- Monitor installation activities
- Monitor any necessary system changes and regression testing
- Verify Implementation Stage Security Activities to include C&A

- Conduct analysis of system metrics
- Monitor execution of system training
- Generate Lessons Learned

3.6.1 Implementation Stage – Document Reviews

The IV&V Team will review documentation delivered during the Implementation Stage. This will include the final program package, Implementation Plan, Training Materials, and production documentation.

Table 3- 38, Implementation Stage - Document Reviews

Task	Description
Method:	<p>The developer will submit the final program package prior to delivering the product to the installation site. The IV&V Team will evaluate the program package, including Final Implementation Plan, User Manuals, Release Version Description Document (VDD), Maintenance and Operations Plan, Data Conversion Plan, Communication Plan, Transition Plan, and Training Plan. The final program package may also include change pages to documentation.</p> <p>The IV&V Team will also evaluate any installation anomaly reports for severity and all resulting software changes to determine the system impact and ensure the correct implementation and distribution of revised documentation. Based on system impact determinations, IV&V tasks may be iterated as necessary to validate the software. In the process of evaluating anomalies and approved changes, the IV&V Team will verify that no unacceptable changes to software performance have occurred. These documents will be reviewed for correctness and consistency. Documents reviewed include Transition to Support materials, training materials, and final maintenance documentation.</p>
Inputs:	Final Program Package, Implementation Plan, Anomaly Reports, System and User Documentation, VDD, Updated Design Documents for maintenance, Training Material, Configuration Inventories, Project Inventory List, SLA, MOUs, Document Review Checklist
Outputs:	Completed Checklists, Findings
IV&V Standard Reference:	Section 2.5.3

3.6.2 Implementation Stage – Transition, Production Walkthroughs and Monitoring

The purpose of the Transition is to plan, manage and complete support readiness activities. The IV&V Team will verify that the LCM Implementation Stage requirements are met. IV&V will review all production materials and participate in the production phone calls and reviews. IV&V will monitor the production activities and provide a recommendation to Federal Student Aid with a recommendation as to whether or not to “Go Live” based on the Implementation Plan Checklist from the Implementation Plan.

Table 3- 39, Implementation Stage - Transition, Production Walkthroughs and Monitoring

Task	Description
Method:	<p>The IV&V Team will review the Production Materials including the project inventory list, schedules, SLA and training materials. In addition, the IV&V Team will review the document library to ensure it contains the latest versions of the controlled documents needed for maintenance. Lastly, IV&V will verify that all executive sign-off elements are addressed.</p> <p>Prior to the completion of the Implementation Stage and executive sign-off, the following exit criteria will be verified by IV&V:</p> <ul style="list-style-type: none"> • Solution has been successfully deployed • Project Inventory List is baselined • LCM security activities are completed and approved • MOUs/SLAs are established and approved • Transition and Training Plan is in place and being executed • Maintenance and Operations Plan is complete
Inputs:	Readiness Materials, Training Materials, Configuration Inventories, Project Inventory List, SLAs, MOUs
Outputs:	Completed Checklists, Findings, Sign-off recommendation
IV&V Standard Reference:	Sections 2.5.2, 2.5.3, 2.5.4

3.6.3 Implementation Stage – Regression Test Monitoring

The IV&V Team will monitor the developer's regression tests for any changes to the system. Once the hardware or the software has been fixed, regression testing must be performed. The IV&V Team will assure all test results are obtained in the approved hardware/software environment. The IV&V Team will verify the implementation of configuration management controls, contingency planning, and anomaly tracking. In addition, the IV&V Team will assess the need for regression testing throughout this lifecycle stage.

Table 3- 40, Implementation Stage - Regression Test Monitoring

Task	Description
Method:	<p>The IV&V Team will observe regression testing and verify successful re-execution of formal procedures. The IV&V Team will verify configuration management procedures are followed through mini-reviews of defect tracking and code control. The IV&V Team will verify that contingency plans are in effect. Regression testing will be observed and any failures during testing will be evaluated. Failures detected will be reviewed to determine why the failure occurred, to identify code and documentation changes, to determine which tests need to be repeated, to isolate changes made to existing tests, and to uncover new tests which must be developed. This analysis will be performed using the following procedures:</p> <ul style="list-style-type: none"> • Observe the repeatability of the test to verify the invalid results. • Ensure that the test failure is documented in the test logs or other documentation with cross-references to any problem reports. • Evaluate the test output with the expected results for possible errors. If the test procedure is in error, a problem report must be generated to correct the documentation error. Testing resumes after successfully repeating the test with the corrected procedure. • When the software is in error, an analysis is necessary to determine whether to halt all testing pending software correction, resume testing using red-lined test procedures, develop new test procedures, or use a work-around that avoids the failed portion. • Follow all of the guidelines required for a formal test activity.
Inputs:	Anomaly Reports, Test Procedures and Results, CM Plans, Process Review CM Checklist
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.5.4, 2.5.9, 2.5.12

3.6.4 Implementation Stage – Installation Configuration Review

At the discretion of Federal Student Aid, IV&V can review the installation of the system to verify that correct versions of software are installed and procedures are followed. The IV&V Team's involvement during installation will include monitoring the system installation and verifying that there is configuration control of the environment and system changes. The IV&V Team will also verify that system cutover plans and contingency planning (fallback positions) exist. The IV&V Team will track lessons learned and capture them in each IV&V Final Report provided to Federal Student Aid.

Table 3- 41, Implementation Stage - Installation Configuration Review

Task	Description
Method:	In support of configuration reviews, a checklist will be generated to ensure that the developer’s plans, products, technical documentation, and reports are formally accepted. This will aid in providing evidence that all the requirements have been satisfied and that the evidence verifies the Configuration Item’s system performance and functionality against its approved configuration documentation. The IV&V Team will provide summary data for all previously completed IV&V activities, ensure that the review follows established standards and published agenda, and assist in the performance of the configuration review.
Inputs:	Final RTM, Transition to Support, Readiness Materials, Configuration Inventories, Project Inventory List, Inventory Checklist
Outputs:	Completed Checklists, Findings
IV&V Standard Reference:	Sections 2.5.3, 2.5.8

3.6.5 Implementation Stage – Security Activities

The IV&V Team must review the results of all security reviews and will ensure that Security requirements are traced through the Business Case, RDM, code and test results. The IV&V Team will continue to work with the assigned SSO and keep him/her abreast of any IV&V security issues.

Table 3- 42, Implementation Stage - Security Activities

Task	Description
Method:	<p>At the end of the Implementation Stage, the IV&V Team will ensure the performance of all security related activities including:</p> <ul style="list-style-type: none"> • Documented completion of Corrective Action Plan (CAP) from Construction And Validation Stage • Completed Security Test Plan • Completed Information Technology Contingency Plan • POA&M Review • Documented Security Test Results • Certification & Accreditation Letter (Approval to Operate or Interim Approval to Operate) • Final System Security Plan • Final Continuity of Operations Plan • Final Disaster Recovery Plan • User Training Schedule • Approved User Access Request Forms

Task	Description
Inputs:	Business Case, RTM, Assignment Letters, Business Partner List, Requirements Matrices, Security Risk Assessment and Mitigation Plan, POA&M Review, Information Technology Contingency Plan, System Security Plan, Integrated Baseline Review
Outputs:	Findings
IV&V Standard Reference:	Sections 2.5.2, 2.5.10

3.6.6 Implementation Stage – Risk Analysis

The IV&V Team will continue to monitor program risks and will maintain a Risk Watch List. The Risk Watch List should be delivered to Federal Student Aid on a regular basis, and the IV&V Team should review all outstanding risks with Federal Student Aid and Development Program Managers.

Table 3- 43, Implementation Stage - Risk Analysis

Task	Description
Method:	The IV&V Team will continue to maintain an independent risk watch list and recommend mitigation strategies. Risk areas will continue to be focused on schedule, cost, performance, future maintenance, training, and staff availability as the project comes to conclusion.
Inputs:	Current Plans, RTM, Test Results, WBS, developer staffing plan
Outputs:	Risk Watch List, findings
IV&V Standard Reference:	Section 2.5.1

3.6.7 Implementation Stage – IV&V Final Report and Lessons Learned Generation

The IV&V Team will prepare an IV&V Final Report.

Table 3- 44, Implementation Stage - IV&V Final Report and Lessons Learned Generation

Task	Description
Method:	During this stage, the IV&V Team will prepare a Final Report documenting all of their findings, including detailed lessons learned. A sample format for this report is included in Section 5.

Task	Description
Inputs:	Risk Watch List, Issue Log, Findings, Lessons Learned Template
Outputs:	IV&V Final Report, Completed Lessons Learned Template
IV&V Standard Reference:	Section 2.5.6

3.6.8 Implementation Stage – IV&V Metrics

The IV&V Team will continue to track metrics during this stage of development and will report any concerns or issues via an MOR or as part of the Risk Watch List, Issue Log, or Weekly Status Report.

Table 3- 45, Implementation Stage - IV&V Metrics

Task	Description
Method:	The metrics during this stage will pertain to system installation, performance and maintenance issues. Typically the IV&V Team will track adherence to schedule, regression test progress, security standards and defect tracking.
Inputs:	Business Case, RTM, WBS, maintenance statistics, support data, Security Documentation
Outputs:	Metrics MOR, or inputs to regular status reporting and risk/issue logs
IV&V Standard Reference:	Section 2.5.6

3.7 LCM Support and Improvement Stage

The System Support and Improvement Stage is the period of time during which Federal Student Aid system upgrade or iteration is evaluated from an operational and maintainability standpoint. The IV&V Team will evaluate the performance of the system and address continued maintenance issues. The team will monitor operational activities and may perform operational site visits to ensure that the system is operating according to plans, procedures and established standards. In addition, the IV&V Team can participate in the Post Implementation Review. The level of participation by the IV&V Team is dependent upon access to the environment. Some of the benefits IV&V provides during this stage are:

- Review updated system documentation
- Operations Reviews
- System enhancements and fixes

- Support Contract Reviews
- Post Implementation Review Support

3.7.1 Support and Improvement Stage – Document Reviews

The IV&V Team will review updated maintenance and support documentation, operational plans and procedures, anomaly reports, applicable regression test results, and the updated contract and Business Cases. Help Desk documentation and updated training materials are also reviewed.

Table 3- 46, Support and Improvement Stage - Document Reviews

Task	Description
Method:	IV&V’s primary focus will be on reviewing maintenance and operational documentation. These reviews include final versions of technical documents, operational procedures, and training documentation. Documents will be reviewed based on the Document Review Checklist. This checklist will be tailored as needed. IV&V will support Federal Student Aid in evaluating any changes in projects costs and/or schedule.
Inputs:	Final Program Package, Anomaly Reports, System and User Documentation, VDD, Lessons Learned, Document Review Checklist
Outputs:	Completed Checklist, Findings, Additional Lessons Learned
IV&V Standard Reference:	Sections 2.3.3, 2.3.11, 2.3.12

3.7.2 Support and Improvement Stage – Post Implementation Review (PIR) Support

The IV&V Team will provide lessons learned and support of the Clinger-Cohen/Office of Management and Budget (OMB) mandated agency level PIR conducted by the Enterprise Quality Assurance Team. A briefing of the IV&V final report can be provided at the discretion of Federal Student Aid. The IV&V Team will assess whether program objectives were met, in addition to evaluating the overall development and management processes. The IV&V Team will monitor system utilization and ensure a problem and change request tracking system is in place and being used effectively.

Table 3- 47, Support and Improvement Stage - Post Implementation Review (PIR) Support

Task	Description
Method:	In support of the Post Implementation Review, the IV&V Team will generate a checklist to verify entrance and exit criteria. The IV&V Team will review metrics and lessons learned prior to the review. The IV&V Team will continue to monitor any outstanding defects and/or risks that may impact the deployed target system and provide feedback to Federal Student Aid. Post Implementation Review Criteria must include assurance that

Task	Description
	project value and success measures have been reasonably met or exceeded.
Inputs:	Metrics, IV&V Findings, Lessons Learned, Tailored Criteria Checklist, PIR Report
Outputs:	Findings, Recommendations
IV&V Standard Reference:	Sections 2.5.1, 2.5.3, 2.5.4, 2.5.6, 2.5.12

3.7.3 Support and Improvement Stage – Security Activities

The IV&V Team will assess the results of all security reviews and will ensure security requirements are traced through the Business Case, RDM and preliminary design. The IV&V Team will continue to work with the assigned SSO and keep him/her abreast of any IV&V security issues.

Table 3- 48, Support and Improvement Stage - Security Activities

Task	Description
Method:	At the end of the Support and Improvement Stage, the IV&V Team will ensure that the Security procedures are being followed and all of the outstanding C&A actions are mitigated. Other security related activities including: <ul style="list-style-type: none"> • C&A Issue Tracking Activities • Documented completion of final test results • Updated Operation Procedures • Regression Testing Results
Inputs:	RTM, Operation Procedures, Test Results, C&A, CAP
Outputs:	Findings
IV&V Standard Reference:	Sections 2.5.2, 2.5.10

3.7.4 Support and Improvement Stage – Risk Analysis

The IV&V Team will continue to monitor program risks and will maintain a Risk Watch List. The Risk Watch List should be delivered to Federal Student Aid on a regular basis and the IV&V Team will review all outstanding risks with Federal Student Aid and Development Program Managers.

Table 3- 49, Support and Improvement Stage - Risk Analysis

Task	Description
Method:	The IV&V Team will continue to maintain an independent risk watch and recommend mitigation strategies. The focus of risk assessment will be performance and operational, as well as reliability and availability issues.
Inputs:	Current Plans, WBS, GFE and/or COTS Technologies Documentation, Business Case
Outputs:	Risk Watch List
IV&V Standard Reference:	Section 2.5.1

3.7.5 Support and Improvement Stage – IV&V Metrics

The IV&V Team will continue to track metrics during this stage of development and will report any concerns or issues via the IV&V Metrics Report or as part of the Risk Watch List, Issue Log or Weekly Status Report.

Table 3- 50, Support and Improvement Stage - IV&V Metrics

Task	Description
Method:	All of the operational performance metrics will be tracked and monitored by IV&V. During this Stage, the metrics continue to focus on system reliability, maintainability and availability (RMA) issues. In addition, requirements will be monitored in terms of future upgrades and enhancement. Help Desk support may also be addressed as part of risk assessment.
Inputs:	RMA statistics, operational support data, review results, performance data, and Help Desk Records
Outputs:	IV&V Metrics Report, or inputs to regular status reporting and risk/issue logs
IV&V Standard Reference:	Section 2.5.6

3.8 LCM Retirement Stage

The purpose of the Retirement Stage is to execute the systematic termination of the system and preserve vital information for future access and or re-activation. The level of participation by the IV&V Team is dependent upon access to the environment. Some of the benefits IV&V will provide during this stage are:

- Review Retirement Plan
- Review System Disposal Plan

- Change Requests
- Integrated Baseline Review Report
- Support technical and program reviews
- Provide updated lessons learned
- Verification of System Archives, storage and data artifacts
- Verification that privacy requirements are met for system data storage

3.8.1 Retirement Stage – Document Reviews

The IV&V Team will review the Retirement and Disposal Plans, review board activities, technical reviews, and storage requirements.

Table 3- 51, Retirement Stage - Document Reviews

Task	Description
Method:	The primary focus will be on Retirement Stage documents including the Retirement Plan and Disposal Plans. Both plans will be reviewed to verify they meet Federal Student Aid requirements, policies and procedures. In addition, license agreements should be reviewed to ensure that they are retired and maintained for retired systems. IV&V will ensure the necessary updates to the CM documents are performed. IV&V will assess the overall retirement planning process.
Inputs:	Retirement Plan, System Disposal Plan, Federal Student Aid Retirement Policies and Procedures, Change Request, Integrated Baseline Review Report, CM Plan, Document Review Checklist
Outputs:	Completed Checklist, Findings
IV&V Standard Reference:	Sections 2.3.3, 2.3.11, 2.3.12

3.8.2 Retirement Stage – Risk Analysis

The IV&V Team will continue to monitor program risks and will maintain a Risk Watch List. The Risk Watch List should be delivered to Federal Student Aid on a regular basis and the IV&V Team should review all outstanding risks with Federal Student Aid and Operation Managers.

Table 3- 52, Retirement Stage - Risk Analysis

Task	Description
Method:	The IV&V Team will continue to maintain an independent risk watch list and recommend mitigation strategies. The issues and risks will be archived as part of the system artifacts. Security risks should be reviewed to ensure that there are no outstanding security or privacy issues with the system and data being retired.

Task	Description
Inputs:	Current Plans, WBS, GFE and/or COTS Technologies Documentation, Contractor and Government Risk Lists, Business Case
Outputs:	Risk Watch List
IV&V Standard Reference:	Section 2.5.1

3.8.3 Retirement Stage – IV&V Metrics

The IV&V Team will continue to track metrics during this Stage of development and will report any concerns or issues via the IV&V Metrics Report or as part of the Risk Watch List, Issues Log or Weekly Status Report.

Table 3- 53, Retirement Stage - IV&V Metrics

Task	Description
Method:	During this Stage, the metrics will focus on planned system retirement activities. Operational Metrics and Help Desk support will need to be archived.
Inputs:	Final operational support data, review results, retirement planning documents, CM Plan updates, Department of Education System Shutdown Policies
Outputs:	IV&V Metrics Report or inputs to regular status reporting and Risk/Issue Logs, Archived Metrics
IV&V Standard Reference:	Section 2.5.6

Section 4. Security Assessment Standards and Procedures

4.1 Overview

This introductory section establishes the purpose and scope of the standards and procedures for evaluating the compliance of Federal Student Aid information systems with Federal information security and privacy mandates, Department of Education and Federal Student Aid Security Policies and Procedures, and the effectiveness of Federal Student Aid information systems security. The Federal Government requires that all of its agencies authorized to hold and/or originate official government information protect that information from unauthorized access, disclosure, modification, manipulation, or destruction regardless of the classification of the material.

For systems identified as General Support Systems (GSSs) or Major Applications (MAs), also called “sensitive systems or applications,” specific assessment standards and Certification and Accreditation requirements apply.

The primary objective of an effective information system security program is to establish, maintain, and periodically evaluate the safeguards to protect information at a level of risk acceptable to management. The vital components of accomplishing that objective are:

- Criticality and Sensitivity Assessments for new systems and applications to determine if they qualify as a GSS or MA
- Security Risk Assessment, mitigation strategy, and residual risk determination for GSSs and MAs that involve review of the completeness, effectiveness, and compliance posture for management, operational, and technical security controls
- A Continuous Monitoring program for all systems and applications in accordance with a security control assessment plan
- Preparation of documents necessary for Security Certification and Accreditation of the GSSs and MAs (“Certification Package”)
- Independent review of the Security or Certification and Accreditation process artifacts and validation of the associated security controls
- Execution of a Security Test and Evaluation (ST&E) as part of the Certification and Accreditation process
- Security Design and Architecture Assessments conducted during the development lifecycle of a system or application
- Performance of a FISMA Self Assessment or independent review of a FISMA Self Assessment
- Review of the adequacy and completeness of Corrective Action Plans (CAP) and/or Plans of Actions or Milestones (POA&Ms)

- Vulnerability Scanning and/or Penetration Testing of networks and applications (including database applications)

Independent assessments associated with the above activities are an integral part of a comprehensive IV&V program for systems throughout their lifecycle to help ensure compliance with the Department of Education's Security Program and all Federal mandates.

The analytical processes for both performing and independently verifying and validating the security lifecycle activities associated with GSSs and MAs and reviewing system functionality and artifacts are discussed in the sections addressing Security Assessments Standards and Procedures.

4.1.1 Scope

The security assessment standards and procedures contained in this section can be applied separately or as a process, depending on the lifecycle stage of the system and needs of the system owner, to ensure that system security is adequately addressed for current Federal Student Aid information systems or systems undergoing development. This section addresses the following security IV&V assessment activities which may include on-site visits to the vendor's sites:

- Assessment of security throughout the system's lifecycle
- Evaluation of security related documentation throughout the system lifecycle (e.g., SDLC, System Security Plan (SSP), security test scripts, requirements, inventory, Disaster Recovery and Business Continuity Plans, and configuration checklists for system devices)
- Emphasis on verification that security controls as outlined in the SSP are adequately implemented in a consistent manner
- Execution or evaluation of Risk Assessments
- Execution or evaluation of Continuous Monitoring programs
- Execution or evaluation of Security Architecture Assessments and assessment of technical controls
- Execution or evaluation of Network Security Assessments
- Execution or evaluation of Vulnerability Scanning and/or Penetration Testing
- Execution or evaluation of Security Program Self Assessments
- Execution or evaluation of Security Test and Evaluations
- Evaluation of Certification and Accreditation Packages
- Evaluation of security-vulnerability remediation packages and evidence
- Preparation or evaluation of Corrective Action Plans/Plan of Actions and Milestones

4.1.2 Assumptions

It is assumed that the Security Assessment Teams will have access to artifacts (documentation, code, tests, devices (e.g., servers), data stores, etc.), facilities, and staff in order to conduct the

various types of system security IV&V assessments. The specific artifacts, facilities and staff can be derived from the standards and procedures contained in this section of the Handbook.

The IV&V Team can be brought in at any phase of the system lifecycle. However, IV&V involvement as early as is practical in the lifecycle, such as during the Vision Stage, will add the greatest value to Federal Student Aid.

It is assumed that all government and contractor organizations and support facilities that are providing critical-service support to the application(s) will make the appropriate security documentation and system(s) available to ensure that a complete analysis and potentially on-site testing can be conducted.

4.1.3 Tailoring

These security assessment standards and procedures may be tailored for the specific target system. Tailoring will be based upon three factors:

- The security architecture or model for the system or application
- The degree to which the system or application relies on security controls provided and managed by other associated systems (e.g., an application may rely on GSS security features and controls)
- The System Security Plan for the system or application

Special conditions related to performing a particular security effectiveness evaluation may dictate other measures to complement these standards and procedures. Such situations and the measures recommended should be documented in assessments or test plans and reports.

4.2 Application of Security Assessment Standards

This section describes the appropriate standards to be used for the various types of Security Assessments. Some of the standards are common to the various forms of security assessments (e.g., risk assessments and security architecture assessments). Others are unique owing to the specialized nature or specific objective associated with the review or analysis undertaken.

In seeking guidance, Department of Education and Federal Student Aid Security Policies and Procedures should first be consulted, as they convey the Department of Education's official policies and procedures against which all systems and applications will be evaluated. Any deviation from Department of Education and Federal Student Aid Policies and Procedures must be documented and approved in writing, typically as part of the accreditation statement for a GSS or MA.

4.2.1 Laws, Regulations, Standards, and Guidelines

The following laws, regulations, standards, and guidelines are key to IV&V security assessments:

- Federal Information Security Management Act of 2002 (FISMA) (Title III of the E-Government Act, Public Law (PL) 107-3479)

- HSPD-7 Homeland Security Presidential Directive, Critical Infrastructure Identification, Prioritization, and Protection (supersedes Presidential Decision Directive (PDD)-63)
- Privacy Act of 1974, PL 93-579, as amended
- OMB Circular A-123 – Management Accountability and Control, 2004
- OMB Circular A-127 – Financial Management Systems, July 23, 1993
- OMB Circular A-130 – Management of Federal Automated Information Resources
- Computer Fraud and Abuse Act of 1986, PL 99-474
- Computer Security Act of 1987, PL 100-235
- Confidential Information Protection Security and Efficiency Act of 2002 (CIPSEA), Title V of PL 107-347
- Electronic Communications Privacy Act of 1986, PL 99-508
- Federal Enterprise Architecture (FEA) Reference Model
- Federal Information Processing Standards (FIPS) Publication (Pub) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- Federal Information Processing Standards (FIPS) Publication (Pub) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- Federal Manager Financial Integrity Act of 1986
- Freedom of Information Act, PL 93-502
- Paperwork Reduction Act of 1980, as amended
- Section 508 of the Rehabilitation Act, as amended

The IV&V Team should be familiar with all of the laws and regulations identified above and reference them accordingly in assessment plans and reports. Additionally, all security guidance, including mandatory Federal Information Processing Standards (FIPS) issued by the NIST Computer Security Division, Computer Security Resource Center, can be consulted at <http://csrc.nist.gov/>.

4.2.2 Security Policy and Procedures

The following are the key information assurance related Department of Education Security Policies, Procedures, and Guides (this information is reproduced from Handbook OCIO-01):

- Baseline Security Requirements, NIST SP 800-53, Revision 2, dated December 2007 should be used as the source of security requirements
- Critical Infrastructure Protection Plan
- Handbook OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures, March 31, 2006
- Handbook OCIO-07, Handbook for Information Technology Security Risk Assessment Procedures, January 13, 2004

- Handbook OCIO-09, Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures, March 16, 2005
- Handbook OCIO-10, Handbook for Information Technology Security Contingency Planning Procedures, July 12, 2005
- Handbook OCIO-11, Handbook for Information Technology Security Configuration Management Planning Procedures, July 12, 2005
- Handbook OCIO-13, Handbook for Telecommunications
- Handbook OCIO-14, Handbook for Information Security Incident Response and Reporting Procedures, May 13, 2005
- Handbook OIG-1, Handbook for Personnel Security-Suitability Program, January 1, 2003
- Information Technology Security Communications Guide
- Information Technology Security Compliance Guide
- Information Technology Security Cost Estimation Guide
- Information Assurance Program Management Plan (IAPMP)
- Information Technology Security System Development Life Cycle Integration Guide
- Information Technology Security Test and Evaluation Guide
- Information Technology Security Controls Reference Guide
- IT Security Metrics Program Plan
- OCIO: 1-104, Personal Use of Government Equipment
- OCIO: 2-102, Wireless Telecommunications Services
- OCIO: 3-106, Information Technology Security Facility Physical Security Policy
- OM: 2-104, Occupant Emergency Organizations and Plans
- OM: 3-104, Clearance of Personnel for Separation or Transfer
- OM: 4-114, Physical Security Program
- OM: 5-101, Contractor Employee Personnel Security Screenings Policy
- OM: 5-102, Continuity of Operations (COOP) Program
- Handbook OM-01, Handbook for Classified National Security Information
- EDNet-POL-000-0128, Use of Laptop Equipment on EDUCATE
- PMI 368-1, Flexiplace Program

The CIO issues guidance to advise Principal Offices on proper implementation of the information assurance program. To obtain the most current versions of these documents as well as any new security policies and procedures published since this handbook was produced; the Department of Education's connectED Intranet site for OCIO/IAS should be consulted (from the connected home page run a search for "the starting line").

The most current version of NIST SP 800-53 can be found at <http://csrc.nist.gov/publications/PubsSPs.html>. Additionally, a security library of policies and procedures related to information security is available via the Department of Education Intranet at http://thestartingline.ed.gov/cio/products/it_security_portal/library.shtml.

4.2.3 Security Assessment Standards

Security and the Systems Development Lifecycle – Assessments of lifecycle management and C&A lifecycles and associated processes should be based on:

- Department of Education, OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures, dated March 31, 2006.
- Department of Education, Administrative Communication System, Departmental Directive OCIO: 1-106, LCM Directive Version 1, dated August 30, 2005.

Security Risk Assessment including assessments of baseline security requirements identified in NIST SP 800-53, Revision 2, dated December 2007, and Criticality and Sensitivity Determinations/Validations should be based on:

- Handbook OCIO-07, Handbook for Information Technology Security Risk Assessment Procedures, January 13, 2004.
- Department of Education Handbook for Information Assurance Security Policy, Handbook OCIO-01, dated March 31, 2006.
- Criticality and Sensitivity Determinations/Validations – the system categorization should be based on the guidance provided in NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories and in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

NIST Special Publication (SP) 800-53, Revision 2, dated December 2007, Recommended Security Controls for Federal Information Systems, supplements the policies contained in Handbooks OCIO-01 and OCIO-07. The appropriate set of security controls (low, moderate, or high) should be used as the “Baseline Security Requirements” (BLSRs) referenced in Handbooks OCIO-01 and OCIO-07.

ST&Es should be based on:

- Information Technology Security Test and Evaluation Guide.
- NIST Standards including NIST SP 800-53A, dated June 2008, NIST Security Configuration Checklist Programs for IT Products which can be found at <http://csrc.nist.gov/checklists/index.html>, and Federal Student Aid Security Configuration Guides.
- Federal Desktop Core Configuration (FDCC) Listing which can be found at <http://nvd.nist.gov/fdcc/index.cfm>.
- Security Content Automation Protocol (SCAP) which can be found at <http://nvd.nist.gov/scap.cfm>.

Assessments of Security Designs and Architectures should be based on:

- NIST Security Configuration Checklist Programs for IT Products (<http://csrc.nist.gov/checklists/index.html>), Federal Student Aid Secure Configuration Guides and standards and guidelines mutually agreed to by the IV&V Team and the Federal Student Aid client organization, as part of determining of the scope of the assessment.
- NIST SP 800-64, Revision 2, Security Considerations in the Information System Development Life Cycle, dated March 14, 2008.
- Section 4.9, Assessment of Security Designs and Architectures, provides additional detailed assessment guidance.

4.2.4 Future NIST Security and IV&V Related Guidelines

NIST is updating, and where sufficient guidance was not available, creating new guidance for Certification and Accreditation, Risk Management, Security Considerations in the SDLC, Technical Security Testing, and Security Performance Metrics. NIST is also updating and altering the terminology and processes associated with the certification and accreditation of systems and applications. The following Security and IV&V relevant NIST Special Publications are undergoing revisions and will be adopted upon their completion by the Department of Education and Federal Student Aid:

- **NIST SP 800-37 Revision 1 – DRAFT Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach, dated August 19, 2008**

This draft document is the result of the completion of an interagency project conducted by NIST to develop a common process to authorize federal information systems for operation. The publication contains the proposed new security authorization process for the federal government (currently commonly referred to as certification and accreditation, or C&A). The new process is consistent with the requirements of the Federal Information Security Management Act (FISMA) and the Office of Management and Budget (OMB) Circular A-130, Appendix III, promotes the concept of near real-time risk management based on continuous monitoring of federal information systems, and more closely couples information security requirements to the Federal Enterprise Architecture (FEA) and System Development Life Cycle (SDLC). The new security authorization process described in this publication transforms the disparate approaches to Certification and Accreditation (C&A) from the various federal communities and creates a common process to authorize federal information systems for operation. As part of the C&A transformation, a unified information security framework has been developed for the federal government and its support contractors that provides a common foundation of information security building blocks including standardized approaches for: (i) categorizing information and information systems; (ii) specifying management, operational, and technical security controls for information systems; (iii) assessing the effectiveness of security controls; and (iv) managing risk. The C&A transformation objectives are four-fold:

- Develop a common security authorization process for federal information systems that can provide the capability of near real-time risk management;

- Express the process of authorizing information systems to operate as an integral part of the SDLC and the Risk Management Framework (RMF);
- Provide a well-defined and comprehensive process that helps to ensure responsibility and accountability for managing information system-related security risks; and
- Incorporate a *risk executive (function)* into the security authorization process to ensure that managing information system-related security risk:
 - Is consistent across the organization;
 - Reflects organizational risk tolerance; and
 - Is performed as part of an organization-wide process that considers other organizational risks affecting mission/business success.
- **NIST SP 800-39 – DRAFT Managing Risk from Information Systems: An Organizational Perspective, dated April 3, 2008**

This draft publication provides guidelines for managing risk to organizational operations, organizational assets, individuals, other organizations, and the nation resulting from the operation and use of information systems. Special Publication 800-39 is the flagship document in the series of FISMA-related publications developed by NIST and provides a structured, yet flexible approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of organizations.

- **NIST SP 800-64, Rev. 2 – DRAFT Security Considerations in the System Development Life Cycle, dated March 14, 2008**

The purpose of this draft revision is to assist federal government agencies in integrating essential information technology (IT) security steps into their established IT system development life cycle (SDLC). This should result in more cost effective, risk appropriate security control identification, development and testing.
- **NIST SP 800-115 – DRAFT Technical Guide to Information Security Testing, dated November 13, 2007**

This draft document was written to assist organizations in planning and conducting technical information security testing, analyzing findings, and developing mitigation strategies. The publication provides practical recommendations for designing, implementing, and maintaining technical information security testing processes and procedures. SP 800-115 provides an overview of key elements of security testing, with an emphasis on technical testing techniques, the benefits and limitations of each technique, and recommendations for their use. Draft SP 800-115 is intended to replace SP 800-42, Guideline on Network Security Testing, which was released in 2003.
- **NIST SP 800-80 – DRAFT Guide for Developing Performance Metrics for Information Security, dated May 4, 2006**

This draft guide is intended to assist organizations in developing metrics for an information security program. The methodology links information security program performance to agency performance. It leverages agency-level strategic planning

processes and uses security controls from NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to characterize security performance. To facilitate the development and implementation of information security performance metrics, the guide provides templates including at least one candidate metric for each of the security control families described in NIST SP 800-53.

The versions and dates of the NIST documents discussed above are current as of the publication of this Handbook. All of the documents identified in this section are drafts, subject to revision, and should not be used as official guidance until they are formally adopted by the Department of Education and/or Federal Student Aid. The following URL should be consulted for the latest versions of all NIST Special Publications including the ones discussed or identified throughout Section 4 of this Handbook: <http://csrc.nist.gov/publications/PubsSPs.html>.

4.2.5 Performance-Based Features

Performance-based security features should be evaluated in accordance with the Department of Education IT Security Metrics Program Plan, dated March 2003. The IT Security Metrics Program Plan contains information on the Department of Education's performance measurement and the steps needed to create and maintain an IT security performance measurement program.

4.3 Security and the Lifecycle Management Framework (LCM)

The following documents should be referred to for guidance pertaining to required security activities and the systems development lifecycle:

- OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures, dated March 31, 2006.
- Federal Enterprise Architecture Reference Model (<http://www.whitehouse.gov/omb/egov/a-2-EAModelsNEW2.html>).
- Department of Education, Administrative Communication System, Departmental Directive OCIO: 1-106, LCM Directive Version 1, dated 8/30/2005.

The beginning of the system lifecycle is the appropriate time to initiate security planning and begin the process of completing all necessary components of the system's security program leading to a successful Certification and Accreditation. An effective security program is planned to ensure that all relevant management, operational and technical controls are completed, tested and implemented in advance of placing the system into operation. In the following sections, the LCM Framework and the phases of the Department of Education's Certification and Accreditation program are referenced as to when certain security related activities should begin in order to increase the likelihood of their effectiveness and enable compliance with Department of Education directives and guidelines.

Exhibit 4-1 indicates when certain security related activities and evaluations would be appropriate. The actual employment of these security activities and evaluations is dependent upon many additional factors including adequately addressing security requirements in contract documents and system development schedules. As proved in past systems development projects, the sooner the security program is formally initiated, security requirements defined, security

vulnerabilities identified, and solutions incorporated in the systems design, the less likely it is that security issues will delay deployment of the system.

Exhibit 4- 1, Security Assessment Activities During the LCM Stages

Security Assessment Activity						
LCM Stage	Critical Infrastructure Protection Questionnaire	Privacy Impact Assessment	E-Authentication Assessment	Security Risk Assessment	Security Architecture Assessment	Security Program Assessment/ Self Assessment
Vision	•					
Definition		•	•	•	•	•
Construction and Validation		Review and update as necessary	Review and update as necessary	•	•	•
Implementation		Review and update as necessary	Review and update as necessary	•	•	•
Support and Improvement		Review and update as necessary	Review and update as necessary	• (Conducted at least every three years as part of C&A during system operating/ production)		•
Retirement						

4.3.1 Vision Stage

During the Vision Stage, the system security function will be assigned to the SSO. The SSO is responsible for planning and administering the system’s security program, managing the C&A process and ensuring that all required security activities and artifacts are produced. In addition, the SSO is responsible for ensuring that the security system’s components are validated throughout the lifecycle through IV&V security assessments, risk assessments, architecture assessments, and vulnerability analysis as described in this document.

During this stage, the following security program components should be identified, produced, and available for review:

- Identification of the C&A Team
- Initial Security Requirements Set
- Critical Infrastructure Protection Questionnaire (CIP)
- GSS or MA Inventory Form

- SOW with the appropriate LCM and security language (if applicable)

Technical reviews and approvals are obtained during the Vision Stage from the OCIOs Technical Review Board (TRB) and Security, Regulatory Information Services (RIS), Information Assurance (IA), and Enterprise Architecture (EA).

4.3.2 Definition Stage

During the Definition Stage the Certification and Accreditation Team should be identified if it was not identified in the Vision Stage. Documentation produced during the Vision Stage should be reviewed and updated as required, and the following security related documents should be produced and available for review:

- High-level security requirements
- Draft C&A Work (or Project) Plan
- Draft system security documentation to include:
 - System Security Plan (SSP)
 - Configuration Management Plan
 - Contingency/Continuity of Support Plan and/or Disaster Recovery Plan (DRP) (if required)
 - ST&E Plan (only required for Tier 3 and 4 systems)
- Draft Privacy Documentation
 - Privacy Impact Assessment
 - Privacy notice for website (if required)
 - System of Record Notice (Privacy Act System of Record) (if required)
 - System of Record Update (Financial System of Record) (if required)
- Draft E-Authentication Risk Assessment
- Initial Risk Assessment and CAP

Technical reviews and approvals continue to be obtained during the Definition Stage from the OCIOs TRB and Security, RIS, IA, and EA. The SSO should participate in refinement of the security budget for the remaining stages based upon system design progress and complexity. An initial schedule for certification and accreditation should also be developed.

During the Definition Stage, the SSO should, in addition to the Initial Risk Assessment, initiate an assessment of the security architecture to determine compliance with the EA as it pertains to security design and use of security middleware software. General Security Assessments can also be performed to determine the effectiveness of the security program and the above components in identifying and mitigating the threats and vulnerabilities attributed to the system and the information stored, processed and exchanged by the target system.

4.3.3 Construction & Validation Stage

During the Construction and Validation Stage, the SSO is responsible for ensuring that: (1) the security initiatives begun in earlier stages are incorporated into the security plan and the appropriate management control and operational control documents, and (2) the security requirements are included in the detailed system design documentation.

Under a fully budgeted IV&V effort, the IV&V contractor will review all security artifacts delivered by the development contractor or organization. As part of the overall IV&V effort, system requirements will be traced to COTS product features/settings and application program test scripts. Under an IV&V risk based approach, IV&V analysts should also monitor the developer's testing of security requirements.

During this stage, the following security-related documents and artifacts are verified and further refined:

- Design level security specifications
- Interface design and connectivity security design documents
- System and security architecture documentation
- COTS products to be acquired and security settings proposed
- Overall project plan to include the C&A Work (or Project) Plan
- Draft system security documentation to include:
 - System Security Plan
 - Rules of Behavior
 - Roles and responsibilities for system users (Trust Matrix)
 - Configuration Management Plan
 - Contingency/Continuity of Support Plan and/or Disaster Recovery Plan (if required)
 - ST&E Plan (only required for Tier 3 and 4 systems)
- Update (as needed) Privacy Documentation and E-Authentication Assessment
- Updated (iterative update) Risk Assessment and Corrective Action Plan

During the Construction and Validation Stage, the SSO should initiate an update (iterative update) to the risk assessment performed in the prior stage to determine if security controls are adequate to counter the previously identified threats and vulnerabilities and if there is adequate progress in addressing prior findings/CAP items. At the same time, architecture assessments conducted earlier should be updated to account for any changes to the design and the security technology employed in the design.

The overall objective in this stage from a security standpoint is to reaffirm the security requirements derived from the business case, trace them to the detail design, and independently assess the overall effectiveness of the target system and its security program prior to freezing the detailed design. All security deficiencies identified in IV&V risk assessments, architecture assessments, and CAPs should be reviewed on a timely basis by the SSO. The SSO's

concurrence with or rejection of those findings and recommended actions should be forwarded to the system manager and/or development contractor for action.

4.3.4 Implementation Stage

During the Implementation Stage, the target system's security features should be configured and enabled. The system (including the security controls) will be tested, authorized for processing, and placed in a production status during this stage. A PRR will be conducted prior to proceeding into production. If additional security controls are identified or previous controls modified during this stage, they will undergo acceptance testing to verify that they are effective and that they do not interfere with or circumvent existing controls.

The Implementation Stage has particular significance because of the requirements found in OMB Circular A-130 and reflected in the Department of Education's Policy. By accrediting and authorizing processing of a target system, the system owner/accrediting authority accepts the risks associated with placing the system into production including the risks of uncorrected risk assessment findings. The system owner/accrediting authority must make the final decision to commence production and relies upon the organization or third party performing the ST&E and making the certification recommendation.

The results of acceptance testing are also a major consideration in recommending the deployment of the system into a production environment. The developer must demonstrate that all security functionality is in place and working properly. In addition, the SSO must complete all requirements for Certification and Accreditation. During the Implementation Stage the following security related reviews, tests, approvals, and documents are produced in final form:

- Production Readiness Review approval
- Final Security C&A documentation set is produced and posted to the appropriate Federal Student Aid "Public Folder." To include Final:
 - Privacy Documentation
 - E-Authentication Assessment
 - System Security Plan
 - Rules of Behavior
 - Roles and responsibilities for system users (Trust Matrix)
 - Configuration Management Plan
 - Contingency/Continuity of Support Plan and/or Disaster Recovery Plan (if required)
 - Security Test and Evaluation Plan (only required for Tier 3 and 4 systems)
 - Risk Assessment (iterative update) and CAP
 - Plan of Actions and Milestones (POA&M)
 - Certification and Accreditation Recommendation

- Final Memorandums of Understanding and service level agreements completed and executed (as required)
- C&A process completed and authority to operate (ATO) or Interim Authority to Operate (IATO) signed

Technical reviews and approvals continue to be obtained during the Implementation Stage from the OCIOs TRB and Security, RIMS, IA, and EA.

4.3.5 Support and Improvement Stage

The Support and Improvement Stage continues through the life of the system. During this stage, the Certification and Accreditation document set is updated as required but at least annually to reflect system modifications. Security documents that are reviewed and updated during this stage include:

- System Security Plan
- Rules of Behavior
- Roles and responsibilities for system users (Trust Matrix)
- Configuration Management Plan
- Contingency/Continuity of Support Plan and/or DRP (if required)
- Testing of the Contingency/Continuity of Support Plan and/or DRP (for Tier 3 and Tier 4 systems and applications)
- Update (as needed) Privacy Documentation and E-Authentication Assessment
- Risk Assessment (iterative update) and CAP
- POA&M (quarterly reports are prepared by the SSO)
- Memorandums of Understanding and Service Level Agreements

During the Support and Improvement Stage the SSO is involved in:

- Security reviews as part of the change control process
- Approval and oversight over system backups
- Participating in training classes
- User registration/deregistration and administration of access privileges
- Evaluation of annual Contingency/Continuity of Support and/or Disaster Recovery tests (for Tier 3 and 4 systems and applications)
- Conducting or coordinating periodic network and/or application server vulnerability scans
- Ensuring that independent risk assessments are conducted periodically or whenever a major system change occurs
- Ensuring that a Continuous Monitoring program is in place and executed according to the Continuous Monitoring Plan for the system or application

- Recertification and Accreditation of the system at least every three years or upon a major system software and/or hardware modification as determined by SSO
- Accreditation of the system at least every three years
- Performing a FISMA self assessment of the system

Annual technical reviews are conducted by the OCIOs TRB and Security, RIS, IA, and EA as determined appropriate during this stage.

4.3.6 Retirement Stage

From a security standpoint, the purpose of the Retirement Stage is to ensure that all sensitive data has been sanitized or destroyed once the system is no longer in service. The SSO is responsible for ensuring that all security activities associated with the shutdown and retirement of the system are in accordance with Department of Education and Federal Student Aid Policy and Guidance. The following policy, procedure, and guidance documents should be consulted for evaluating Retirement Stage system decommissioning activities:

- ED Handbook OCIO-01, Handbook for Information Assurance Security Policy
- Federal Student Aid General Support System and Major Application Backup Media Handling Policy
- ED Property Management Manual, Office of Management Facility Services, dated December 2002
- NIST SP 800-88, Revision 1, Guidelines for Media Sanitization, dated September 2006

Additionally, Federal Student Aid has developed the following annotated plan templates associated with the Retirement Stage of a system:

- Federal Student Aid System Retirement Plan, Version 0.1, dated July 12, 2007 (annotated template)
- Federal Student Aid System Disposal Plan, Version 0.1, dated July 12, 2007 (annotated template)

A Federal Student Aid System Disposal Checklist Template is provided in Appendix G and should be completed as part of the system retirement process.

4.4 Security Assessment Methodology

In general, three types of security assessments are performed in the course of development and maintenance of an application or system. They are:

- Security Risk Assessment (including iterative assessments during the development lifecycle)
- ST&Es
- Assessments of Security Designs and Architectures

Additionally, Continuous Monitoring is performed during the maintenance phase for the application or system.

In order to maintain independence the IV&V Team or contractor should not perform both the security risk assessment and ST&E. Assessments of security designs and architectures may be requested at any point of the development lifecycle of the system or application. The purpose of these design and architecture assessments is to help Federal Student Aid manage risks by having an independent assessment and opinion regarding in-house or third party system development projects.

As part of security risk assessments, vulnerability scanning and/or penetration testing should be performed. Vulnerability Scanning and penetration testing is addressed in Section 4.10, Vulnerability Scanning and Penetration Testing. ST&Es are discussed in Section 4.6, Security Test and Evaluation.

Assessments of Security Designs and Architectures, Security Risk Assessments, Security Architecture Assessments, and Security Program Self Assessments involve an evaluation of a target system's management, operational, and technical security controls. The results of the review establish a baseline for planning remediation activities and measuring their results. The type and rigor of review is commensurate with the Tier Rating (i.e., Tiers 1 through 4 with 4 being the most critical/sensitive level), stage of the system in the LCM, the maturity of the security program under review, the acceptable level of risk established for the system, and the likelihood of gaining useful information to improve security.

The benefits of a security assessment are not completely achieved unless the results are reported to the appropriate managers who can take actions needed to improve the security program. Such actions may include:

- Reassessing previously identified risks
- Identifying new problem areas
- Reassessing the appropriateness of existing controls and security related activities
- Identifying the need for new controls
- Monitoring recommended follow-up actions
- Redirecting subsequent assessment activities
- Holding managers accountable for compliance

Security Risk Assessments should be conducted in accordance with the Department of Education Handbook for Information Technology Security, Risk Assessment Procedures, dated January 13, 2004 (Handbook OCIO-07). NIST SP 800-53, Revision 2 should be the basis of the assessment along with Department of Education Security Policies and Procedures. The Department of Education Secure Configuration Guides, dated February 2008 or the NIST Security Configuration Checklist (<http://csrc.nist.gov/checklists/repository/category.html>), should be used to assess specific software platforms. The SSO and/or the IV&V Team can recommend additional security controls or countermeasures based on identified vulnerabilities not effectively mitigated by NIST Security Controls and the Department of Education's Security Policies and Procedures. For all of these references it is assumed that subsequent updates of these standards apply as well.

4.4.1 Approach and Preparation

The guidance for conducting assessments is derived primarily from the Department of Education's Policies, Procedures, and Guidance documents, OMB Circular A-130, NIST SP 800-30, NIST SP 800-53, Revision 2, NIST SP 800-53A, FIPS 199, and the practices employed by the IV&V Team based on past experience with Government IT Security assessments, C&A, and Government best practices. In addition, the IV&V Team should be provided the target system's security policy and security plan that will assist in establishing the scope and emphasis of the assessment.

A security assessment is organized into three phases:

- Security assessment planning, coordination, and document acquisition
- Security assessment site review
- Analysis and reporting

Once an assessment plan has been prepared and approved, a coordination meeting is held to establish the overall scope of the effort. It identifies the points of contact within the program organization, SSO office and the technical staff. Subsequently, an interview schedule is prepared and coordinated. The interview questions are based on FISMA and NIST SP 800-53.

An initial effort involves a detailed scoping of the target system and the programmatic environment it supports. A security assessment project typically involves a characterization of the threats profile of the application, and the risks or consequences of a threat successfully exploiting a system vulnerability where a NIST SP 800-53, Revision 2 security requirement is not met.

In addition to examining the presence of security artifacts and controls, the assessment will seek to determine if controls are operating as intended. In addition, as part of the interview process, the security assessment team will evaluate the effectiveness of the security program in communicating policies, raising awareness levels, and reducing incidents.

4.4.2 Security Assessment Team (SAT) and Resource Requirements

The IV&V or third party/contractor security assessment teams should be comprised of cleared, (cleared at 6c level in accordance with the Department of Education requirements), experienced and certified security engineers and analysts that are familiar with:

- Designing, testing, and reviewing security and internal controls for large scale Government financial systems
- All Department of Education Security and Privacy Policy, Procedures, and guidelines
- All Federal security related mandates
- OMB Circulars
- OMB Memorandums
- GAO financial system audit guidance (e.g., FISCAM)
- NIST Special Publications (SPs) and other NIST guidance documents

- FIPS documents
- National Security Agency (NSA) guidance for operating system/platform configuration and information security assessments/vulnerability scanning
- The application of Government and commercial best security practices for financial systems

IV&V security and privacy assessment teams should be comprised of certified and experienced professionals with each key security engineer/team member holding at least a Certified Information Systems Security Professional (CISSP) certification. Other desired certifications include:

- Certified Information System Auditor (CISA)
- Certified Business Continuity Professional (CBCP)
- Certified Information Security Manager (CISM)
- National Security Agency INFOSEC Assessment Methodology Certification (NSA-IAM)
- National Security Agency INFOSEC Evaluation Methodology Certification (NSA-IEM)
- Certification in use of forensics software
- Other vendor certifications in security software products and middleware

In addition, IV&V contractors with a business focus of IT security and IV&V are desirable. Contractors should be able to provide evidence of completing numerous successful C&A processes that reflect the structure and discipline of successful IV&V and QA methodologies. It is desirable for a prospective IV&V contractor to have successfully supported both CIO and Inspector General (IG) organizations for security and assessment tasks.

The IV&V contractor should also have experience in performing FISMA assessments and demonstrate that their risk assessments and C&A work products have successfully sustained IG audits.

4.5 The Risk Assessment Process

This section discusses the risk assessment process including the methodology, the content of the risk assessment report, forms associated with risk analysis, and the evaluation of the risk assessment report.

4.5.1 Risk Assessment Methodology

The Federal Student Aid risk assessment methodology is a qualitative, requirements based format that is NIST SP 800-30 compliant. Any automated risk assessment tools proposed for use to conduct Federal Student Aid system or application risk assessments must comply with Department of Education and Federal Student Aid methodology requirements and be approved prior to use.

A Risk Assessment is required to be conducted as an integral part of the C&A process and is intended to, in part, assure that Management, Operational, and Technical controls are functioning

correctly and effectively. The type and rigor of the assessment should be commensurate with the acceptable level of risk established for the system, budget, and time constraints set for the project and the likelihood of learning useful information to improve systems security.

The Risk Assessment report documents the security assessment activities performed by the assessment team over a given period of time and in addition to fulfilling a C&A requirement helps Federal Student Aid management understand the current security posture of the System or application and its risk exposure.

System Risk Assessments must be compliant with the following Department of Education policies, procedures, guides, and requirements documents:

- Handbook OCIO-07, Handbook for Information Technology Security Risk Assessment Procedures, January 13, 2004
- NIST Standards including NIST SP 800-53A, NIST Security Configuration Checklist Programs for IT Products, and Federal Student Aid Security Configuration Guides

Risk Assessments are conducted throughout the lifecycle of a system or application. A system under development, especially one being developed and deployed in multiple phases, will require several iterative risk assessments. Table 4-1, System Development Lifecycle (SDLC) Stages and Related Risk Assessment Activities provides guidance on risk assessment activities that should be performed during each SDLC stage. It has been reproduced from the Department of Education’s Risk Assessment Procedures and modified to reflect the most current Department of Education SDLC. At a minimum, for a system in production, a risk assessment must be performed at least every three years. **All risk assessments should be marked and treated as “sensitive” documents in accordance with Department of Education Procedures.**

Table 4- 1, SDLC Stages and Related Risk Assessment Activities

SDLC Stage	Risk Assessment Activity
Vision	Risks are identified to ensure security controls are being considered and will be built into the GSS or MA. Conduct a high-level risk assessment using the appropriate set of NIST 800-53, Revision 2 security controls as a checklist to ensure security controls are being considered and will be built into the GSS or MA.
Definition	The risks identified during this stage are used to support the development of the systems requirements, including security requirements.
Construction and Validation	<p>A GSS or MA Inventory submission form must be submitted to the OCIO during this stage. This will assess the anticipated mission criticality and information sensitivity of the system.</p> <p>Examination of the construction and validation stage is performed to ensure that the business case, project plan, and risk management plan are followed.</p> <p>Decisions regarding risks identified must be made prior to the Implementation Stage. During this stage, an independent risk assessment that meets the minimum standards of these procedures (the Department of Education’s Risk Assessment Procedures) must be performed.</p>

SDLC Stage	Risk Assessment Activity
Implementation	The risk management process supports the assessment of the GSS or MA implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to the system Support and Improvement Stage.
Support and Improvement	It is good practice to perform a risk assessment during the Support and Improvement Stage of the GSS or MA—in anticipation of the occurrence of an event or even after the occurrence of an event—to analyze vulnerabilities and recommend remediation measures.
Retirement	Risk management activities are performed for GSS or MA components that will be retired or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that migration is conducted in a secure and systematic manner.

Risk Assessments for Federal Student Aid systems or applications should contain the following information:

- **Executive Summary** – contains an overview, purpose, and background discussion of the assessment and the system. The findings should be grouped by risk level (i.e., high moderate, low) and summarized at an appropriate level of detail for the Federal Student Aid executive audience. Detailed technical discussions should be avoided.
- **Introduction** – contains a summary discussion of the risk assessment methodology, and identifies document sensitivity and applicable distribution and reproduction controls. The introduction should also provide the following information:
 - **Background** – a moderately detailed description of the system or application under assessment (e.g., software, hardware, networks, facilities, characterization of users) including the lifecycle state of all subsystems or system components assessed.
 - **Assessment Roles and Responsibilities** – a description of the owner or responsible organization for the system, business functions and organizations associated with the system. All Federal Student Aid, contractor and other third party personnel that were interviewed for the assessment and contributed information should be identified by name, title, and organization.
 - **Purpose** – the purpose of the report should be discussed in brief, its function in supporting the C&A process for the system or application, and the Department of Education and legislative mandates it addresses.
 - **Scope** – the scope of the assessment should be discussed to include the systems, applications, networks, facilities, and business organizations and functions supported.
 - **Report Organization** – a brief annotated outline of all of the report sections including the appendices should be provided.
- **Risk Assessment Approach** – a detailed discussion of the assessment approach to include identification of relevant Department of Education Policy and Procedures,

legislative mandates and guidance sources consulted and applied (e.g., Handbook OCIO-07, OMB Circular A-130, NIST SP 800-30, NIST SP 800-53, Revision 2, FIPS 191, FIPS 199, FISMA). The steps followed in the assessment process should be described and include the following sections:

- **Definition of System Boundaries** – an explanation of the process used to define and bound the system or application assessed.
- **Information Gathering Procedures** – a description of the methods used to gather information for the assessment (e.g., interviews, emails, site visits, documentation reviews, and vulnerability scanning).
- **Conducting the Risk Assessment** – the key subtasks of the assessment process should be described including how the security controls were selected, threats identified, vulnerabilities identified, risks determined and rated, and countermeasures/recommendations developed.
- **Review of Findings And Observations** – a description of the process of presenting a draft findings report to the Federal Student Aid client, the findings validation process, and presentation of observations (control or process areas recommended for improvement that do not currently represent finding).
- **Threat Statement** – a description of the applicable threat sources, the threat actions and agents (actors), and a detailed discussion of the threat profile. Depending on the scope of the assessment, the security controls should be discussed by using NIST Control Objectives as described in NIST SP 800-53, Revision 2.
- **System Identification** – this section should contain the following information:
 - System Name/Title
 - Responsible Organization
 - Information Contact(s)
 - Assignment Of Security Responsibility
 - Other Key Points Of Contact
 - System Operational Status
 - System Environment
 - System Interconnection/Information Sharing
 - Applicable Laws Or Regulations Affecting The System
 - General Description Of Criticality and Sensitivity
- **Summary of Findings** – this section should contain a NIST SP 800-30 compliant findings statement, grouped according to management, operational, and technical controls. This summary should be in the form of either a narrative or a matrix and this is determined by the SSO. The SSO would typically review and approve an outline for the risk assessment. Each statement should contain:
 - Statement of the threat/vulnerability (finding)

- Description of the potential impact of the finding
- Capability (high, moderate, low)
- Likelihood (high, moderate, low)
- Effectiveness of countermeasures (high, moderate, low)
- Assessment of the of the level of risk to Federal Student Aid based on the threat and vulnerability assessment and impact of any existing mitigation mechanisms or controls
- The countermeasure recommendation that would reduce or eliminate the risk

Typically the following appendices should be included with the report (as required):

- This appendix should contain the security control set used for the assessment (i.e., NIST SP 800-53, Revision 2; low, moderate, or high security controls; and any additional or special security requirements)
- **Risk Assessment Findings Matrix** – this appendix should contain a NIST SP 800-30 compliant findings matrix that includes for each finding (grouped according to control objective):
 - Description of the vulnerability (finding)
 - Threat category
 - Impact description
 - Impact Calculation (high, moderate, low)
 - Capability (high, moderate, low)
 - Effectiveness of countermeasures (high, moderate, low)
 - Likelihood (high, moderate, low)
 - Risk (high, moderate, low)
 - Priority (high moderate, low)
 - Description of proposed countermeasures (recommendations)
- **Document Request Log** – this appendix should contain a listing and description of all documents requested, obtained, and reviewed in support of the assessment.
- **Acronyms** – this appendix should contain a listing and description of all acronyms used in the document.
- **Vocabulary** – this appendix should contain a listing of definitions for all specialized terminology used in the document.
- **Document Review Comment Resolution Form** – this section should contain all comments received on the draft document and information on their resolution.
- **Evidence** – this section should contain (if determined necessary) detailed notes extracted from work papers that support analysis leading to particular findings.

The Department uses an online system called Open Vulnerability Management System (OVMS), and certain information gathered and recorded in the Risk Assessment report will need to be entered into OVMS. OVMS will be used to generate Corrective Action Plans/Plans of Actions and Milestones and to track and manage all findings associated with the system Risk Assessment.

4.5.2 Evaluating the Risk Assessment Report

Evaluation of a Risk Assessment report is similar to the evaluation of a Security Architecture Assessment or Security Test and Evaluation report. The following are the key elements of a Risk Assessment report that should be evaluated by an IV&V Analyst:

- At a minimum, the Risk Assessment should address the appropriate NIST SP 800-53, Revision 2 security controls applicable to the system or application.
- Outline and Scope – the development of an outline and scope for the risk assessment should contain the information described in Section 4.5.1 - Risk Assessment Methodology, and scope should be approved by the SSO, System Owner, OCIO, and IA.
- Threat Profile – the description of the threat profile for the system should be complete and address all NIST Control Objectives. Both effective and deficient control areas should be addressed. The assessment should demonstrate that the analyst understands the difference between a threat, vulnerability, and risk.
- System identification – the characterization and description of the system or application should be complete and accurate and boundaries/scope of the assessment clearly defined. The criticality and sensitivity should be calculated in accordance with FIPS 199 in order to determine the correct NIST SP 800-53, Revision 2 security controls (i.e., low, moderate, high) to apply. The assessment should demonstrate that the analyst understands the difference between criticality and sensitivity. Diagrams depicting the system and all interfaces and interconnections should be included in the report.
- Analysis and findings – the analysis should be qualitative and findings and recommendations presented in clear business language that are mapped to the security controls. All ratings and calculated values should be in accordance with the Department of Education's Risk Assessment Procedures. If automated tools are used the IV&V Analyst should verify that the tool performs risk related calculations correctly.
- Execution of the risk assessment in accordance with the Department of Education's Risk Assessment Procedures – the documentation of risk assessment findings should be clear, accurate, and understandable/readable by both business and technical personnel. For each finding clear recommendations should be provided such that if followed by the system owner the finding would be resolved. An out brief should also be conducted prior to delivery of the Final Risk Assessment report in order to allow the SSO, system owner, and other system or application officials to provide comments and have the opportunity to correct and/or eliminate incorrect or inappropriate findings (i.e., findings not traceable to applicable requirements).
- Continuous Monitoring – Whether or not a risk assessment is conducted during the year, Continuous Monitoring is necessary to ensure that the system's security is not degraded:

1. Increase the monitoring of the audit logs for privileged users to minimize the impact of unauthorized or unintentional changes to processes and/or user privileges;
2. Target the monitoring of security controls that were identified as vulnerabilities in the last risk assessment to ensure continued compliance with the remediation of the vulnerability;
3. Adjust the monitoring of security controls to comply with new Office of Management and Budget memorandums, for example (OMB M06-17); and
4. Every year, select a subset of security controls to monitor for training purposes and to ensure continued compliance with the documented security controls procedures.

Additionally, the system security plan should be reviewed annually to validate that the documentation of the security controls is consistent with the system's current operational technical, and management procedures.

4.6 The Security Test and Evaluation (ST&E) Process

Section 4.6, Security Test and Evaluation, provides an overview of the ST&E process and identifies the applicable Department of Education Policy and Guidelines for performing ST&Es.

ST&E is performed during the Validation (Phase 3) of the C&A process. An ST&E is an independent test and evaluation of the management, operational, and technical security controls over a system or application undergoing C&A. ST&E is a validation of the accuracy and completeness of the risk assessment and the artifacts of the C&A package.

An IV&V Analyst may be involved in reviewing the ST&E process applied for a system or application C&A to verify and validate the completeness and accuracy of the ST&E provided they were not involved in preparing and conducting the risk assessment for the system.

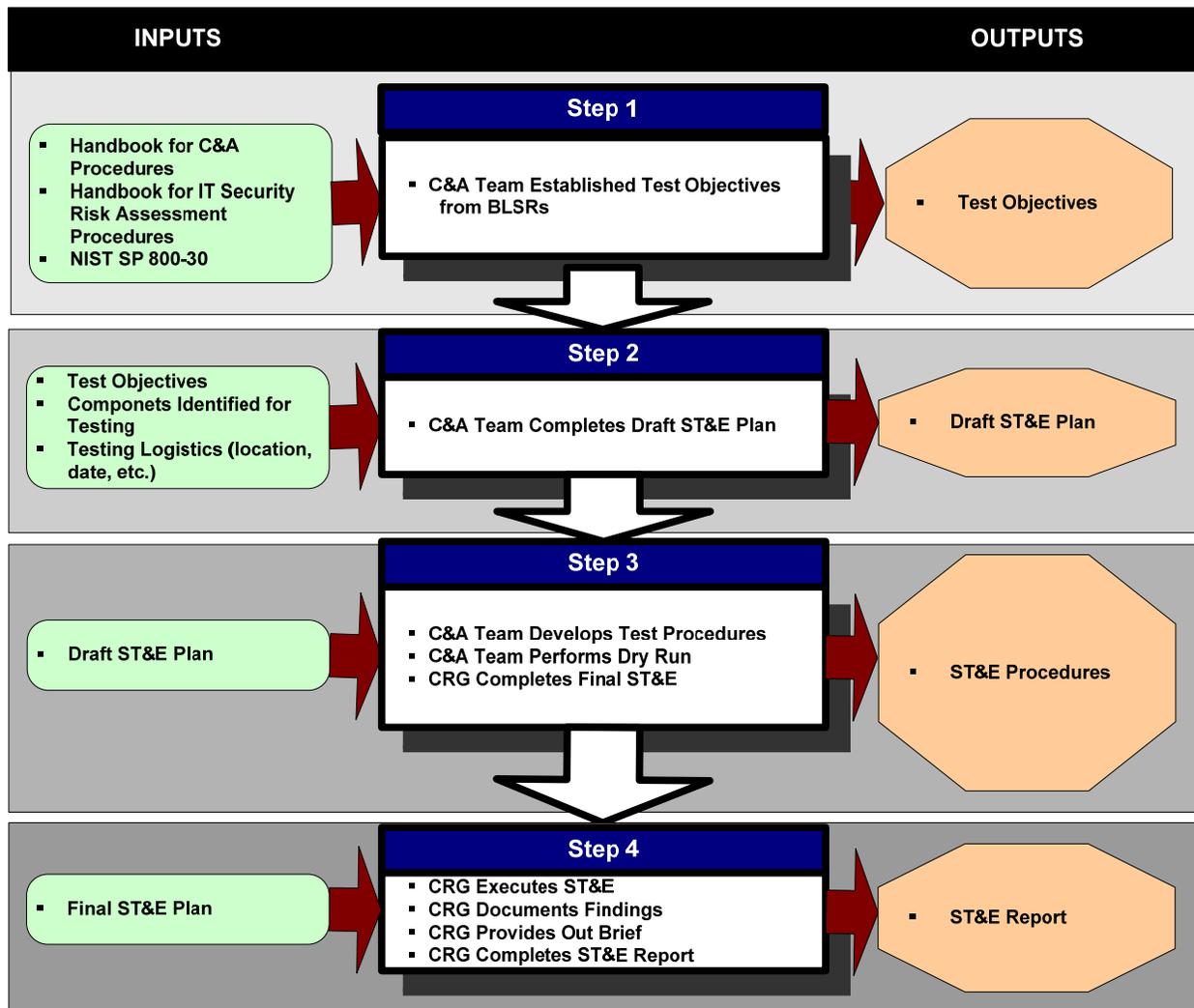
4.6.1 Security Test and Evaluation (ST&E) Methodology

The Department of Education's methodology for conducting ST&E involves a four step process as follows:

- Step 1 – Preparation of Test Objectives
- Step 2 – Preparation of a Draft ST&E Plan
- Step 3 – Development of ST&E procedures
- Step 4 – Preparation of an ST&E Report

The process, its inputs, activities, and outputs are depicted in Figure 4-1, ST&E Methodology, reproduced from the Department of Education's Information Technology Security Test and Evaluation Guide.

Figure 4- 1, ST&E Methodology



4.6.2 Evaluating the Security Test and Evaluation (ST&E) Report

Evaluation of an ST&E report is similar to the evaluation of a risk assessment or security architecture assessment. The following are the key elements of an ST&E that should be evaluated by an IV&V Analyst:

- Establishment of Test Objectives for the ST&E – Test objectives should be based on, or traceable to, the appropriate set of NIST SP 800-53, Revision 2 security controls. An initial set of test objectives can be found in Appendix D of the Department of Education’s ST&E Guide. Other sources for test objectives/test requirements include:
 - Federal Student Aid, Secure Configuration Guides, dated February 2008
 - Configuration Guides available via the NIST Security Configuration Checklist Program

- Development of an outline and scope for the ST&E – the outline and scope should be approved by the SSO and System Owner.
- Development of ST&E Procedures for each test in accordance with the Department of Education’s ST&E Guide – the test procedures for each test should be evaluated to determine if they are in fact applicable to the system or application undergoing ST&E. Inappropriate test procedures can lead to erroneous findings that can be difficult to eliminate after the testing has been completed.

Execution of the ST&E and development of an ST&E Report in accordance with the Department of Education’s ST&E Guide – the documentation of findings should be clear, accurate, and understandable, and readable by both business and technical personnel. For each finding clear recommendations should be provided such that if followed by the system owner the finding would be resolved. An out brief should also be conducted prior to delivery of the Final ST&E Report in order to allow the SSO, system owner, and other system or application officials to provide comments and have the opportunity to correct and/or eliminate incorrect or inappropriate findings (i.e., not traceable to applicable requirements).

4.7 The Security Certification and Accreditation (C&A) Process

C&A is the periodic, independent verification and validation that existing risk management has been effectively implemented. All GSSs and MAs must undergo certification at least every three years or whenever a significant security relevant system change occurs. The Department of Education, Information Technology Security, Certification and Accreditation Procedures (Handbook OCIO-05), dated March 31, 2006, convey the Department of Education’s policy and guidance pertaining to the certification and accreditation process. The Department of Education’s C&A is a four-phased process with the following phases:

- Definition
- Verification
- Validation
- Post-Accreditation

A system or application developed and deployed in multiple phases requires an independent determination of the requirement for certification and accreditation for each deployed phase. The four-phased C&A process will be repeated for each deployed phase requiring C&A.

4.7.1 Overview of Security Certification and Accreditation (C&A)

Certification is an independent comprehensive assessment of the management, technical, and operational controls over a system or application. It involves the review of the C&A “package,” that is, the C&A documentation set that includes the security plan, configuration management plan, contingency/continuity of support and/or disaster recovery plan, risk assessment, and corrective action plan. A certification recommendation is made by an independent or third party performing an ST&E of a system or application undergoing a C&A process. An accreditation recommendation is typically also made by the party performing the certification.

Accreditation is the formal declaration by the Designated Approving Authority (DAA) that the information system is approved to operate using a prescribed set of in place and/or planned safeguards or controls. The DAA should consider the risk assessment, ST&E, and certification recommendation when making risk acceptance decisions and granting an ATO, an IATO, or deny accreditation because of security risks unacceptable to the DAA.

4.7.2 The Certification Package

The certification package is typically comprised of the following documents:

- System Security Plan
- System Risk Assessment
- Configuration Management Plan
- Continuity of Support/Contingency Plan and/or Disaster Recovery Plan (DRP)
- Security Test and Evaluation (ST&E)
- Certification Statement/Recommendation
- Accreditation Statement
- Corrective Action Plan or Plan of Actions and Milestones

The specific content and scope of the System Risk Assessment, Continuity of Support/Contingency Plan and/or DRP, and ST&E generally increases in detail in accordance with the Tier Score (i.e., 0 through 4, with 0 requiring no C&A and Tier 4 representing the most critical and sensitive systems or applications). For further detail, refer to The Department of Education, Information Technology Security, Certification and Accreditation Procedures, dated March 2006, for additional information on the contents of the C&A package.

4.7.3 Evaluating the Certification Package

The most important consideration for the IV&V Analyst in evaluating the Certification Package is documentation that accurately and completely represents both the “in place” and “planned” security controls. The documentation set must also comply with the Department of Education’s and Federal Student Aid’s policies, procedures, and guidance.

4.7.3.1 System Security Plan (SSP)

A GSS or MA SSP is the key document of the C&A package. It documents the management, operational, and technical security controls of the system and should accurately reflect all “in place” and “planned” security control over the system. The SSP should also reference other documents where additional detail of all security controls can be found. Such documents typically include:

- Design documents
- Requirements documents
- Programmer, maintenance, administrator, and user documentation
- Memorandums of Understanding (MOU)

- Service Level Agreements
- Interconnection Agreements
- Documents defining user roles and responsibilities
- Contingency Plans
- Risk Assessments
- Corrective Action Plans

A SSP must be compliant with:

- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems

Responsibilities of each individual who operates or has access to the GSS or MA must be described within the SSP. The SSP is a living document that is periodically updated throughout the lifecycle of the system or application. The IV&V Analyst should consider a poorly written (e.g., inaccurate or lacking details) or deficient SSP as a symptom of systemic deficiencies in the overall security program for the system.

4.7.3.2 System Risk Assessment

Risk Assessments should be a requirements-based qualitative assessment that use NIST SP 800-53, Revision 2, security requirements and Department of Education Security Policies and Procedures as the basis for the assessment. Risk Assessments should be evaluated for compliance with Department of Education and NIST Guidelines for Risk Assessment (NIST SP 800-30).

For a system under development an initial risk assessment should be performed followed by successive iterations of the Risk Assessment for major functionality deployments (or successive phases of development). The System Owner and SSO, in consultation with the Federal Student Aid Chief Security Officer (CSO) and OCIO, determine the need for a risk assessment for a particular system deployment or successive phases of development based on the significance of the deployment (major or minor). If a particular system or application deployment or phase of development is determined to require Certification and Accreditation then it must have a Risk Assessment.

System Risk Assessments must be compliant with:

- Handbook OCIO-07, Handbook for Information Technology Security Risk Assessment Procedures, January 13, 2004

The Risk Assessment should apply a consistent approach to identifying threats, vulnerabilities, and risks. The threat discussion or threat profile for the system or application should be customized and applicable to the actual system in order for the IV&V Analyst to develop appropriate additional security countermeasures (if required) beyond the NIST security requirements.

For all findings clear and complete recommendations for implementing safeguard or remediation measures should be provided. The recommendations should be written at a level understandable by both the technology as well as the business professional. All findings should be associated

with one or more requirements. Poorly or inappropriately supported findings are indicative of a deficient assessment.

The accuracy of the system description and description of the assessment or C&A boundary usually provides a good indication of the quality and completeness of the overall assessment.

Table 4-2, Required Level of Effort for Risk Assessment, reproduced from the Department of Education's Handbook for Information Technology Security, Risk Assessment Procedures (Handbook OCIO-07) provided information on the scope of a Risk Assessment as determined by the Tier rating for the system or application.

Table 4- 2, Required Level of Effort for Risk Assessment

Certification Tier	Required Level of Effort for Risk Assessment
0	No risk assessment required
1	Risk assessment (using NIST SP 800-53A as a checklist)
2	Risk assessment (using NIST SP 800-53A + additional system specific security requirements)
3	Risk assessment (using NIST SP 800-53A + additional system specific security requirements + vulnerability scanning recommended)
4	Risk assessment (using NIST SP 800-53A + additional system specific security requirements + vulnerability scanning)

Performance and evaluation of vulnerability scanning is discussed in Section 4.10, Vulnerability Scanning and Penetration Testing.

4.7.3.3 Configuration Management Plan (CMP)

CMPs must be compliant with the following Department of Education policy and procedure:

- Department of Education, Administrative Communication System, Handbook for Information Technology Security, Configuration Management Planning, Version 4.0, dated July, 12, 2005 (Handbook OCIO-11)

A CMP must be developed for each Department of Education GSS and MA to provide configuration management and change control for the system software, firmware, hardware, and documentation throughout the system lifecycle. The IV&V Analyst should ensure an adequate configuration management program and change control process is in place during all phases of the systems development lifecycle. An adequate configuration management program and change control can be evidenced by an adequate CMP with in place and verifiable processes including:

- Defined and documented roles and responsibilities
- Formal methods of communication of configuration changes and change requests
- Defined and documented configuration control process
- Use of tools to manage the system configuration and change requests

- Establishment of a documented configuration baseline
- Establishment of a CM library to maintain all system change request (CR) records
- Use of appropriate forms and electronic documents to initiate, evaluate, approve, and implement system changes
- Periodic configuration verifications and reviews

4.7.3.4 Continuity of Support/Contingency Plan

Continuity of Support/Contingency Plans and DRP must be compliant with the following Department of Education policy and procedure:

- Department of Education, Administrative Communication System, Handbook for Information Technology Security, Contingency Planning Procedures, dated July, 12, 2005 (Handbook OCIO-10)

The Handbook OCIO-10 is based on NIST SP 800-34, Contingency Planning Procedures for Information Technology Systems. This publication should be consulted for additional guidance in assessing contingency planning documents such as continuity of support and disaster recovery plans.

The Department of Education uses the term “Continuity of Support Plan” to refer to short-term IT Contingency Plans or plans to address service interruption scenarios lasting less than 48 hours and not requiring relocation to alternate facilities, and “IT Contingency Planning” to refer to the whole process. NIST guidance uses the terms “Continuity of Support Plan” and “IT Contingency Plan” synonymously.

Adequate contingency planning (to include continuity of support and disaster recovery plans as required) ensures that a GSS or MA can be reconstituted following a disruption of operations. All GSSs and MAs are required to have a continuity of support plan that addresses non-catastrophic disruptions that do not require relocation to an alternate site. Catastrophic disruptions that require alternate sites must be addressed in a DRP. DRPs are only required for Tier 3 and 4 GSSs and MAs. The Department of Education has chosen to work without Tier 1 and 2 GSSs and MAs in the event of a catastrophe, due to their lower mission criticality and data sensitivity.

DRPs are necessary for reacting to major, usually catastrophic, events that deny access to the normal facility for an extended period. A DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of a Continuity of Support Plan. The DRP is focused on long-term outages (over 48 hours) that require relocation to an alternate processing site. Generally, a DRP is produced for a data center or central processing facility in addition to individual application Continuity of Support Plans if required based on system criticality and data sensitivity.

The IV&V Analyst should first evaluate Contingency Planning documents (i.e., Continuity of Support/IT Contingency Plans, DRP) to determine if they are in compliance with Department of Education and NIST guidance. Additionally, Contingency Plans should be evaluated to determine:

- Adequate integration with the Department of Education’s Continuity of Operations Plan (COOP)
- Accuracy of call trees, operational, management, and technical assessment, declaration, recovery, and restoration procedures
- Feasibility of the plans given available resources and training levels of personnel
- Adequacy of testing of the plans and ability to restore and roll forward the system from backup media (table top exercises should not be considered adequate for Tier 3 and 4 systems in production)

All testing of Contingency Plans should be documented through formal test plans approved by the system owner and the SSO. Test results should also be evidenced via documented test reports. Any issues or problems encountered during testing should be formally documented and shared with the system owner.

4.7.3.5 Security Test and Evaluation (ST&E)

ST&E plans, procedures, and reports must be compliant with the following Department of Education policy and procedure:

- Department of Education, Information Technology Security Program, Information Technology Security Test and Evaluation Guide, dated June 2003

The following Department of Education guidance document can be used as an additional source of ST&E test requirements and procedures for Windows, Sun Solaris, Microsoft SQL Server, Oracle, Cisco Router, Open VMS, and mainframes platforms:

- Department of Education, Secure Platform Configuration Guide, dated August 2004

Table 4-3, ST&E Levels of Effort by Certification Tier, reproduced from the Department of Education’s Information Technology Security Test and Evaluation Guide, provides information on the ST&E level of effort as determined by the Tier rating for the system or application.

Table 4- 3, ST&E Levels of Effort by Certification Tier

Certification Tier	Required Level of Effort for an ST&E
1	No ST&E required
2	No ST&E required
3	ST&E (using Test Objectives + additional system specific test objectives)
4	ST&E (using Test Objectives + additional system specific test objectives + penetration testing and automated vulnerability scans)

Tier 3 and 4 GSSs and MAs are required to have an ST&E Plan executed and a Test Report prepared prior to certification. An ST&E is performed to validate the effectiveness of security controls. Specifically, an ST&E is performed to validate the System Risk Assessment and compliance with Department of Education security and privacy policy, procedures, and requirements.

The ST&E process is centrally managed by the Department of Education's Certification Review Group (CRG) or may be delegated to the SSO. If the IV&V entity was involved in preparation or executing the System Risk Assessment they should not be performing or evaluating the ST&E. An ST&E Plan should be developed and tailored to adequately test the management, operational, and technical controls in place for the system or application. Technical tests should also be developed for the specific operating systems and devices comprising the system under review (e.g., UNIX, Windows 2000, Cisco routers).

The objective of the ST&E Plan is to develop a thorough baseline for evaluating the entire security profile of the GSS or MA. The ST&E Plan consists of specific test objectives derived from:

- The applicable NIST SP 800-53, Revision 2 Security Controls for the system
- Tests identified in the Department of Education's ST&E Guide
- Platform and/or device specific tests derived from Federal Student Aid's Secure Configuration Guides
- NIST Security Configuration Checklists

The ST&Es will be executed by the CRG, SSO, or other independent party as determined by the OCIO. When preparing or evaluating ST&Es it is important to note that the primary purpose of the ST&E is to determine the accuracy and adequacy of the C&A documentation set (the C&A Package) including the completeness of the Risk Assessment. ST&E test results should be documented in an ST&E Report and all findings should be supported by and traceable to Department of Education and system security requirements.

4.7.3.6 Certification Statement/Recommendation

The CRG, SSO, or other independent party who executed the ST&E will document the ST&E results in the ST&E Report, which will serve as supporting documentation for the CRG (or SSO or other independent party) recommendation to the Certifier as to whether the Certifier should grant or deny the certification. The Chief Information Officer serves as the Certifier for all GSSs and MAs not under their direct control. The Chief Operating Officer for the Office of Federal Student Aid serves as the Certifier for all GSSs and MAs under the direct control of the CIO.

The party conducting the ST&E should formally document the certification recommendation along with any findings and recommendations resulting from execution of the ST&E in the OVMS.

4.7.3.7 Accreditation Statement

The responsibilities of the Certifier include making both a certification decision, and an accreditation recommendation based on certification recommendation provided by the CRG or other party conducting the ST&E. One of three certification decisions will be made by the Certifier and provided to the DAA:

- If the Certifier finds that the security posture of the GSS or MA is commensurate with the security requirements, the corrective action plan is acceptable for outstanding findings, and residual risks are acceptable, the Certifier will grant certification and recommend full accreditation.

- If the Certifier finds that the security posture of the GSS or MA is not commensurate with the security requirements (e.g., in the case of excessive or high/medium risk outstanding findings or an unacceptable corrective action plan), but short-term operation is commensurate with the Certifier's risk tolerance/acceptance and/or the system is essential for the Department of Education to complete its mission, the Certifier may grant certification and recommend IATO. The IATO enables the system to "officially" operate within a given time constraint (no longer than 3 months) until safeguards are adequately addressed and the system can be reassessed.
- However, if the Certifier finds that the security posture of the GSS or MA is not adequate and operation is not in the best interest of the Department of Education, the Certifier will deny certification. When this occurs, the Certifier will meet with the SSO, C&A Team, CRG, and the DAA to discuss solutions for bringing the system to an acceptable level of security.

After determining certification, the Certifier will provide the DAA with the system security documentation (C&A package), a formal certification decision statement, and accreditation recommendation.

The DAA will make an accreditation decision based on the impact of the residual risk to the Department of Education and whether the DAA is prepared to accept the financial and legal responsibility for the consequences that may occur as a result of their decision. One of three accreditation decisions will be made by the DAA and provided to the CIO:

- If the DAA determines that the residual risk for the system is within an acceptable level, the DAA may grant full accreditation.
- If the DAA determines that the system has deficiencies, but operation of the GSS or MA is essential to fulfill the mission of the Department of Education, the DAA may grant an IATO. The IATO enables the system to "officially" operate within a given time constraint (no longer than 3 months) until safeguards are adequately addressed and the system can be reassessed.
- If the DAA deems the security posture of the system to be inadequate, and determines that operation of the GSS/MA is not in the best interest of the Department of Education, the DAA may deny accreditation.

Upon making an accreditation decision, the DAA will provide the CIO with the decision and accompanied final system security documentation (C&A Package) and an accreditation statement.

Principal Officers serve as the DAA for systems within their purview. Each DAA is responsible for reviewing the certification decision and accreditation recommendation along with the system security documentation for their respective GSSs and MAs.

4.7.3.8 Corrective Action Plan

The CAP is produced after the entry of finding, threat, vulnerability, and countermeasure effectiveness information into OVMS. Section [4.x], OVMS Processes, addresses the 8 step process for resolving findings. All system findings and associated mitigation activities are managed via OVMS. The SSO should use information from the CAP to populate, adjust, and update the POA&M that is submitted by the SSO to the Federal Student Aid CIO.

4.8 OVMS Processes and the Performance Improvement Plan Portal

Findings or Weaknesses / Vulnerabilities identified by Security Assessments, Security Testing and Evaluations, or other audits/assessments must either be accepted as a “business risk,” or a plan to remediate the issue must be developed. Regardless of the disposition, all findings are entered into OVMS. This process involves the following steps after a finding or weakness/vulnerability has been published/issued/declared:

Table 4- 4, OVMS 8 Step Process

OVMS 8 Step Process		
1	Initial Entry of Finding	The finding is entered into OVMS and can be updated with a Course of Action by an authorized contractor or the SSO for the system or application.
2	Entry of Threats and Countermeasures	Threat and countermeasure information is entered for each finding by an authorized contractor or the SSO for the system or application.
3	Entry of Corrective Action	Corrective action information is entered for the findings by an authorized contractor or the SSO for the system or application.
4	SSO Approval	The SSO for the system or application approves the mitigation strategy and other information pertaining to the finding.
5	Gathering of Evidence	The authorized contractor or SSO gather evidence for finding closure.
6	Upload of Evidence	The authorized contractor or SSO upload finding closure evidence.
7	Approval of Evidence	The SSO reviews and approves (or rejects) finding closure evidence.
8	QA Team and IV&V Management Committee Review	The QA Team and the IV&V Management Committee review and accept or reject the finding closure evidence for each finding.

All forms and reports necessary for entering and managing findings, evidence, and approvals are generated by OVMS. The CAP/POA&M is also generated by OVMS.

4.8.1 Recommendation for Closure Forms (RFC)

The Performance Improvement Plan (PIP) Portal is currently a repository for NIST Self Assessments and Critical Infrastructure Protection (CIP) surveys. The PIP Portal is expected to migrate into the Cyber Security Asset Manager (CSAM) database in the first quarter of Fiscal Year 2009. The NIST Self Assessments and CIP surveys are not maintained by OVMS, and there is no integration or duplication of information between the PIP Portal and OVMS. The SSO for a system is responsible for creating and updating the NIST Self Assessment and CIP

maintained in the PIP. The PIP Portal information is not directly relevant to IV&V, but the IV&V vendor should be familiar with this Portal as an information repository.

4.9 Assessment of Security Design and Architectures

Assessments of security design and architectures address systems that are “under design” or “as-built” to determine compliance with requirements, vulnerabilities to selected risks, and deficiencies in requirements. Assessments are normally conducted separate from a risk assessment and can be conducted to validate assessments conducted by contractors or third parties. Findings and any corrective actions from earlier assessments should be addressed. Ratings of finding severity or risks are qualitative (i.e., low, medium, or high risk levels). NIST SP 800-30 should be used as a guide to help determine risk levels. The approach for assessment of security designs and architectures described in this section is based on National Security Agency (NSA) Information Security Assessment Methodology (IAM). The approach can be used to conduct an assessment or verify the completeness of an assessment performed by a third party. The NSA IAM can be applied as a best practice.

4.9.1 General

The areas that should be addressed in assessments of security design and architectures include:

- Adequacy of security and privacy requirements (for systems undergoing design)
- Compliance with contractual documents, the Department of Education’s Policies and Procedures and the Department of Education/Federal Student Aid’s EA
- Technical controls and design features necessary to secure the system, network, and/or application
- System and network Interfaces
- Network design and controls
- External Interfaces
- Custom and COTS Software
- Management and Operational Controls as they impact the security design

The actual areas addressed depend on the scope of the assessment as agreed to by the client Federal Student Aid organization and approved by the system/application SSO or other Federal Student Aid official as required.

Assessment begins with an examination of the technical controls, that is, the security features of the target system that operate automatically, requiring no human intervention. The assessment will document areas not compliant with the Department of Education’s requirements and government best practices depending on the agreed upon scope.

4.9.2 Evaluating Technical Architecture Controls

The evaluation of technical architecture controls involves assessment of security and privacy requirements, system interfaces, network design and controls, external interfaces, custom and

COTS software, management and operational controls assessment, architecture risk calculations, and providing recommendations.

4.9.2.1 Technical Architecture Controls

This section specifies the security assessment approach for assessing the technical aspects of the target system or application architecture.

4.9.2.2 Security and Privacy Requirements

Security and Privacy requirements are typically evaluated for a system under development at various stages of the system's development lifecycle. Guidance for evaluating security requirements during the lifecycle phases is provided by the following Department of Education document:

- The Department of Education, Administrative Communication System, Lifecycle Management (LCM) Directive Version 1, dated 8/30/05, (Handbook OCIO 1-106)

Refer to Section 4.3, Security and the Systems Development Lifecycle for information on the development and refinement of security requirements during the SDLC.

- Privacy Impact Assessments / P3P Requirements

The E-Government Act of 2002 is a new mandate to maintain/increase the integrity with which public information is handled by the government. Section 208 requires Federal Student Aid to complete a Privacy Impact Assessment for each system that collects information in identifiable form about the general public.

During the Definition Stage of the Lifecycle, the SSO must ensure that the team completes the attached Privacy Impact Assessment Questionnaire and must file the completed form in the system's Security Notebook as part of the system's documentation. The electronic copy of the completed form should be stored in the system's Security Folder.

4.9.2.3 System Interfaces

System interfaces are considered internal to the application environment of the target system. For each interface, the assessment should examine the levels of trust as manifested in the permissions and access shared among the processing components.

Most applications and operating systems come with services that may weaken security.

The assessment should examine interfacing components for unused but enabled services in order to prevent this situation.

Another possible consideration in assessment of system interfaces is the workstations. The assessment should determine whether adequate workstation hardening has been performed to mitigate threats that could exploit these components of the system.

MOU and/or SLAs for the internal interfaces should also be examined. The assessment should determine whether security is adequately addressed in light of the known threats/vulnerabilities to the type and protocol of the interface.

4.9.2.4 Network Design and Controls

The assessment should examine the security features of the physical network structure as well as the logical connections for the target system. As a minimum, the assessment should review the

number and location of firewalls and routers, as well as their configuration settings, to assess appropriateness to the threat environment.

Where the physical network features are not adequate to counter the known vulnerabilities/risks, the assessment should examine connection policies, as well as access authorization procedures and other management and operational controls, for supplementary support.

4.9.2.5 External Interfaces

External interfaces include those accessed by the user to organizations outside of Federal Student Aid (e.g., Treasury). The assessment of the user interface depends on the system model. For example, if the system is public, accessible via the World Wide Web, then the assessment will examine web site security banners, password features, link controls, etc. For user access via dedicated LAN/WAN, identification, authorization, and access level features should be reviewed.

The security of interfaces with each external organization should be specified in a documented and formal certification from that organization (i.e., Interconnection Security Agreements and Trusted Party Agreements). The assessment should examine each certification to ensure that adequate protection is in place as reflected in the certification and is compliant with the Trusted Internet Connections (TIC) Capability Form.

The protection of transmitted information should be examined. For example, the Privacy Act of 1974 requires that sensitive data be encrypted if transmitted over non-dedicated or non-private circuits. Additionally, Section 203 of the E-Government Act may require a system to complete an E-Authentication Risk and Requirements Assessment.

4.9.2.6 Custom and COTS Software

The assessment should examine all custom and COTS software products employed by the target system. This should include, as a minimum:

- Compliance with the security requirements
- Adequacy of testing of the software and logical design
- Determination of security risks introduced or exacerbated by use of COTS products
- Review of the COTS security features
- Proper configuration of the software security-related parameters
- Developer's process for managing COTS upgrades, licenses, etc.

The ability of Federal Student Aid or its contractors to maintain and obtain vendor security support for COTS software that has been customized or modified should be examined.

4.9.2.7 Management/Operational Controls Assessment

Management and Operational controls are procedures that are generated through policy, regulations, and written requirements. They are generally implemented and monitored manually and require dedicated persistence to ensure continued effectiveness.

Management and operational controls are not the primary focus of the assessment. However, where technical controls do not adequately abate known risks, the assessment must look to management and operational controls for risk mitigation.

4.9.2.8 Architecture Risk Calculations

The assessment should use Exhibit 4-2, Security Architecture Risk Calculations, to summarize the findings (potential vulnerabilities) of the assessment.

Exhibit 4- 2, Security Architecture Risk Calculations

Findings (Potential Vulnerabilities)	Probability of Occurrence	Potential Impact	Severity of Impact	Residual Risk	Existing or Potential Countermeasure	Department of Education/Federal Student Aid Requirement and/or NIST Requirement Reference
	Low, Medium or High	Low, Medium or High	Low, Medium or High	Low, Medium or High		

- The **Findings (Potential Vulnerabilities)** column is a list of findings identified during the assessment of the target system. The assessment will also include findings identified in prior assessments.
- For each threat/vulnerability, the analysis should list the corresponding **Probability of Occurrence, Potential Impact, and Severity of Impact** in the second, third and fourth columns. If they were determined for particular findings or types of findings during a Security Risk Assessment, then those values should be used. Otherwise, the IV&V Analyst should estimate them using their professional experience and judgment.
- The assessment should determine the **Residual Risk** for each threat. This residual risk accounts for all technical and management and operational **countermeasures** that have actually been or could be readily implemented (listed in last column). Since the residual risk represents the actual remaining risk to the target system security, it is of foremost importance. Therefore, IV&V must bring all of their experience with, and knowledge of, the Federal Student Aid organization to bear on the residual risk calculation.

4.9.2.9 Recommendations

The assessment should recommend additional measures to help abate the residual risks that are deemed medium or high. The assessment should not limit its recommendations to technical controls. Any management and operational control deficiencies or compliance gaps should also be identified. Where feasible, the assessment should identify alternative countermeasures for consideration by Federal Student Aid.

The assessment should consider cost, schedule, and organizational impact when determining potential countermeasures. To this end, the assessment will emphasize countermeasures that can mitigate more than one residual risk.

4.9.3 Evaluating the Four Aspects of Network Defense

No networked system can be fully secured through reliance only on protective controls. Network Security Assessments should address how effectively the system's management, operational, and technical controls implement a defense in-depth strategy that includes protective, detective, responding, and sustaining controls. These controls and the areas that should be assessed are described in the sections below.

4.9.3.1 Protecting

Protecting the network and associated devices and stored data involves hardening and securing of components and systems. The key aspects of protection are maintaining the system configuration according to Department of Education/Federal Student Aid Policy and an adequate and implemented system configuration management program and plan.

Adherence to authoritative configuration guidance (e.g., guidance provided by Department of Education/Federal Student Aid, NSA, NIST, and/or vendors) and remediation management practices which involve implementing vendor patches, hotfixes, and other security and integrity related software and firmware updates should be evaluated.

Certain controls are protective in nature and serve to complement configuration management and remediation management practices. In particular the following control areas should be considered when evaluating network protection:

- Identification and Authentication
- Session Controls
- System Assurance
- Networking
- Malicious Code Prevention
- Communications Security
- Media controls
- Labeling
- Physical Environment
- Personnel Security

Remediation Management controls and procedures associated with patches, hotfixes, and virus signature updates should be evaluated.

System Configuration controls and procedures associated with permissions, access control lists, privileges, passwords, and permitted system services and open ports should be evaluated.

4.9.3.2 Detecting

Detection involves the ability to identify anomalous network or system activity through implementation of audit mechanisms in accordance with Department of Education/Federal Student Aid Policy and Guidelines.

Detective controls that should be evaluated include the use of auditing features and capabilities. The implementation of network auditing associated with intrusion prevention and detection

systems, firewalls, and host based intrusion prevention and detection systems should be evaluated.

4.9.3.3 Responding

Responding involves the ability to report and react to anomalous activity through preplanned reactive measure in accordance with Department of Education/Federal Student Aid Policy and Guidelines.

Response controls that should be evaluated include the incident response plan and procedures, contingency and disaster recovery plans and procedures, and reactive measures documented in help desk and/or standard operating procedures for the system or application.

When evaluating contingency plans particular attention should be paid to how these plans address human intentional and unintentional threat scenarios that impact system integrity, and/or availability (e.g., scenarios where a network or servers are damaged and/or disabled).

4.9.3.4 Sustaining

Sustaining involves the ability to maintain a proper security level through mature processes for system, application, and/or network management in accordance with Department of Education/Federal Student Aid Policy and Guidelines.

Sustaining Controls span all areas of security including management, operational, and technical controls. In particular, the following control areas should be considered when evaluating sustaining network controls:

- Documentation
- Roles & Responsibilities for operation of the network
- Configuration Management
- Account Management
- Maintenance
- Education & Training
- Network Management
- Patch Management Processes
- Group Policy Administration
- Role-based Policies
- Mandatory Access Control implementation (if required)

4.9.4 Recommendations

In conducting an assessment or evaluation of a security design, architecture, or network architecture a formal report should be created and contain (as applicable) the sections and content as discussed below. The recommendations should be entered into the OVMS after all other items are entered.

When evaluating reports produced by other parties the criteria should be the same as those for preparing the report. The section order and or naming is less important than the relevant content of the report.

4.9.4.1 Executive Summary

The executive summary should contain the following information:

- An overview of the organization/mission
- The purpose and methodology of evaluation
- The system description/information criticality
- The major findings and recommendations

4.9.4.2 Introduction

The introduction should provide the background information pertaining to the evaluation and contain the following information:

- An overview of the organization's mission
- The purpose of the evaluation
- Discussion of the organization's information criticality
- Discussion of the system criticality and sensitivity
- Information on the rules of engagement (for vulnerability scanning or penetration testing) including a discussion of customer concerns, constraints, and detailed system information
- References to detailed technical data that is included as an Appendix or on CD

4.9.4.3 Information Security Analysis

This section discusses the technical areas assessed and provides the technical details of the assessment scope:

- The system boundaries associated with the assessment
- External exposures (technical scope of the assessment)
- Internal exposures (technical scope of the assessment)

4.9.4.4 Findings

- Include Common Vulnerability Exposure (CVE) number if applicable
- Medium level of detail for system administrator level
- Organized by customer preference as specified in the Rules of Engagement (ROE)
- Low level findings left in detailed technical data description
- Discuss how & why it is a finding to the customer (is it a security requirements compliance issue)
- Mission impact based decisions and current mitigations
- Includes a list or a table of affected system components

4.9.4.5 Recommendations

- Multiple solutions as available
 - Patch, upgrade, filter, enhance, etc.
- Deliver the level of detail as defined by the customer

4.9.4.6 Conclusion

- Overall security posture description
- Recognition of good security practices and controls

4.9.4.7 Appendices

The appendixes should contain information that would disrupt the flow of the report or information too lengthy for the report main body. Information typically suitable for the appendixes includes:

- The ROE for a vulnerability scan or penetration test
- Detailed technical data such as scan results (on CD if necessary)

4.10 Vulnerability Scanning and Penetration Testing

This section provides information on how an IV&V Analyst should assess (or perform) the planning, execution, and reporting of vulnerability scanning and penetration testing activities. The information in this section is based in part on the NSA Information Security Assessment and Evaluation Methodologies (IAM/IEM). The purpose of this section is to explain a complete vulnerability scanning and penetration testing process that should be followed (i.e., provide a benchmark process against which scanning and penetration testing activities can be assessed for accuracy, completeness, and quality). The process described in this section is designed to address the three phases of scanning or penetration testing (pre-scan activities, on-site activities, and post-scan report preparation).

While technical information is discussed in this section it is not intended to explain all of the details and provide all of the knowledge necessary to perform a vulnerability scan or penetration test. An assumption is made that the IV&V Analyst and/or the party performing the vulnerability scan or penetration test has the required technical knowledge, experience, tools, and certifications necessary to perform the work.

Pre-Scan Activities

The planning of a vulnerability scan or penetration test should include the following activities:

- Review of the most recent risk assessments and vulnerability scan reports for the system.
- For an uninformed (a test where the customer provides little or no information about the network or system to be tested) penetration test, more detailed information on the customer network architecture should be gathered from publicly available information.

- Coordination with the customer organization to determine the ROE.
- Definition of the system and network boundary (scope) of the testing and identification of restricted nodes or components.
- Negotiation on the use of specific tools.
- Definition of customer expectations, constraints, and concerns.
- Identification of any legal requirements associated with the scanning or penetration testing and obtaining legal approval/authorization.
- Identification of any third party connections or leases that may be affected by the scanning or penetration testing.
- Development of a Technical Evaluation Plan or Test Plan and an outline for the Test Report. The contents of the Test Report should be agreed upon prior to performing any scanning or penetration testing.

A Technical Evaluation Plan or Test Plan should be developed and include:

- Points of contact for the test team and customer
- A methodology overview that addresses:
 - Methodology for the testing
 - The ROE
 - Configuration of tools
 - The goals of the testing
 - How testing will be performed
- A description of the systems to be tested
- Detailed network information to include:
 - Physical and logical boundaries (as applicable)
 - Identified subnets and internet protocol (IP) addresses
 - A point of contact in case a critical component is impacted by the testing
- Identification of any customer concerns and their resolution
- Identification of customer imposed constraints
- The ROE which should include:
 - What testing will be done externally and internally
 - Test team requirements
 - Network connections
 - IP addresses
 - Physical space required

- Scan windows
- IP addresses/subnets to test
- Customer technical contact
- Customer requirements
 - IP addresses used by the test team
 - Contact information for the test team
 - Required testing notifications (e.g., customer CIRC point of contact)
 - Identification of the tools and scanning rule sets to be used
- Information on the level of detail to be provided in the recommendations and all deliverables to be provided
- Signature page or Letter of Authorization
- Schedule of events to include the agreed upon scan windows and report delivery dates

Adequate planning will help ensure customer concerns and constraints are addressed and documented. The information gathered and agreements reached during the Pre-Scan Activities should be documented in the Test Plan, Test Report and the ROE as required. Customer “buy-in” on the ROE must be obtained and documented via a signed Letter of Authorization (LOA) for starting the scanning/penetration testing. The LOA should refer to the ROE and Test Plan for detailed information on the scan or penetration test. Every effort should be made to limit impact (including adverse impact) on the customer as a result of the scanning/penetration testing.

On-Site Activities

In addition to performing the actual scanning and/or penetration testing the following on-site activities should be performed:

- An in-brief should be conducted with the customer before starting the scanning or penetration testing.
- The Test Plan should be reviewed and the points of contact confirmed.
- The required physical and logical access should be obtained from the customer prior to the start of the scanning and/or penetrating testing to include:
 - Physical and/or logical access to networks
 - Facility access and workspace (if required)
 - Check-in and inventory of any equipment or software that will be brought to the customer site

Any high risk vulnerabilities identified should be shared with the customer as soon as practical. If work was conducted on-site an out-brief on critical/high risk findings should be provided. The schedule to complete the Draft and Final Test Reports should be reviewed along with any planned meetings to review and/or confirm findings.

Post Evaluation Activities

The post evaluation activities should include:

- Provide the customer, in a timely manner, a Test Report containing an understandable technical analysis of all vulnerabilities identified.
- Provide a customer comment and review period and incorporating comments in the Final Test Report.
- The Test Report should provide complete findings for the evaluation and multiple levels of recommendations to resolve each vulnerability.

An exit briefing should be provided as well as follow-up support for the customer to provide answers to questions or concerns.

4.10.1 Approach

The approach for a vulnerability scan or penetration testing should include the preparation of a ROE document and a LOA. Signature and approval of the ROE and/or LOA by all parties involved is required. In addition, the scope of the testing should be agreed upon and documented in the Test Plan, ROE, and LOA.

4.10.1.1 Rules of Engagement (ROE) including Letter of Authority (LOA)

The ROE should be evaluated to determine if they adequately cover:

- The level of invasiveness of the scanning/penetration testing
- The rule set or specific set of vulnerabilities and services that the scanning will attempt to identify
- The extent (if any) of denial of service testing to be performed
- Timeframes for testing
- Notification or “cut out” procedures in the event of a problem
- Identification of IP addresses to be used for vulnerability scanning or penetration testing
- The level of detail to be provided in the Test Report and Recommendations
- Legal approval from all parties involved
- Signature of the ROE or LOA by all parties involved

4.10.1.2 Setting the Scope of Scanning/Testing (including Third Party Connections and Systems)

All parties involved or affected by the vulnerability scanning and/or penetration testing must be contacted and identified in the ROE and LOA to prevent any misunderstandings including identification of the vulnerability scans or penetration testing as a criminal activity.

Unanticipated third parties may be affected by scanning or penetration testing and must be notified and involved in the preparation of the ROE. Third parties can include:

- Contractors or other government agencies hosting applications or providing network facilities or services

- Other Department of Education or Federal Student Aid applications hosted on the same servers or network segments as the ones being scanned

Not informing and involving third parties in the scan or penetration testing planning and agreement process can expose the Department of Education and/or contractors to litigation risks and potential liability for damages.

4.10.2 Technical Evaluation Activities

This section identifies the baseline activities and potential (example) tools that may be used to perform vulnerability scanning and/or penetration testing. Not all of these activities will be performed for every system, nor will they necessarily be performed in the order discussed. In the absence of Department of Education standards for comprehensive vulnerability scanning this handbook applies the National Security Agency (NSA) Information Security Assessment/Information Security Evaluation (IAM/IEM) methodology as an authoritative guide.

4.10.2.1 Port Scanning

Port scanning is used to identify available or enabled network services on systems and can help identify the existence of unauthorized services or system backdoors. Any open port is a potential way into the system. Examples of port scanners include Nmap, FScan, Superscan, and Solar(w)inds.

4.10.2.2 SNMP Scanning

Simple Network Management Protocol (SNMP) scanning can help enumerate devices on the network and identify community strings if it is enabled. Any information provided by a network and its devices can be used to aid in penetration of that network and/or compromise of its devices. SNMP is a service that provides such information. Examples of SNMP scanners include SNScan, and Solar(w)inds.

4.10.2.3 Enumeration & Banner Grabbing

Enumeration and banner grabbing can be used to identify devices on a network and services listening on their active ports. Examples of tools that can be used for enumeration and banner grabbing include Nmap, Netcat, Fscan, Superscan, Nessus, Saint, and ISS.

4.10.2.4 Wireless Enumeration

Wireless enumeration can help identify wireless access points and potential vulnerabilities of such points including lack of identification and authentication, broadcast of the Service Set Identifier (SSID), rogue file sharing systems, and deficient encryption solutions such as Wired Equivalent Privacy (WEP). Examples of wireless enumeration tools include Kismet, Netstumbler, Airopeek, and AirSnort.

4.10.2.5 Vulnerability Scanning

Vulnerability Scanners can help identify well-known vulnerabilities on network devices such as workstations, servers, and other devices. Examples of vulnerability scanning tools include Nessus, Saint, ISS, and Retina.

4.10.2.6 Host Evaluation

Host evaluation tools can help analyze configuration, access controls, and policy setting for host operating systems. Comparisons to configuration standards recommended by NIST and NSA

can be made. Examples of host evaluation tools include Center for Internet Security (CIS) benchmark tools, and Microsoft Baseline Security Analyzer.

4.10.2.7 Network Device Analysis

Network device scanners can help identify well-known vulnerabilities and insecure configurations in the network security architecture. Examples of network device analysis tools include Router Audit Tool (RAT), Refense, and tools provided by Cisco.

4.10.2.8 Password Compliance Testing

Password compliance testing can help evaluate adherence to password policy and determine whether password policy filters are being effectively implemented. Examples of password compliance testing tools include John the Ripper, L0PhtCrack, ISS, Saint, NetRecon, and Crack.

4.10.2.9 Application Specific Scanning

Application scanning involves the use of automated tools to help identify application vulnerabilities such as those in an Oracle Database Applications or Web based applications. Examples of application scanners include AppDective, Watchfire AppScan, and WebInspect.

4.10.2.10 Network Sniffing

Network Sniffing tools can help identify sensitive information passing through a network such as login credentials and other passwords, and server configuration sessions conducted in the clear with Telnet or other clear text protocols. Examples of tools used to conduct network sniffing include Snoop, Dsniff, Sniffer, Tcpdump, Snort, and Ethereal.

4.10.2.11 War Dialing

War Dialing is an invasive technique to identify exploitable analog access (i.e., dial-up access) via the public switched telephone network (PSTN). Any unsecured or unauthorized/uncontrolled rogue modem connected to a workstation or any device on a network can potentially be exploited to gain control over a network and its resources and data. An example of a tool that can be used for War Dialing is Sandstorm Enterprises PhoneSweep.

4.10.2.12 Denial of Service

Denial of service testing involves testing that can cause system downtime and damage to network devices and corruption or loss of data. Numerous scanning and enumeration tools described above can be used to execute denial of service attacks against networks and their attached devices such as routers, servers, and workstations. The execution of denial of service attacks in the course of vulnerability scanning or penetration testing does not provide valuable insight into security posture. All networks and devices have some vulnerability to denial of service attacks.

4.10.2.13 Penetration Testing

Penetration testing is an invasive technique to exploit vulnerabilities identified through use of the techniques and tools described above. Penetration testing can involve techniques that include denial of service as a way to gain control over a system that is caused to fail in an unstable or unsecured state (e.g., use of a buffer overflow attack to obtain a command prompt for a database or operating system).

The risk of system downtime, damage to servers, and data loss is high for any attempts to exploit vulnerabilities. All parties involved in the penetration test should document such risks and resolve liability issues for damage or losses resulting from the testing in the ROE and/or LOA.

The use of penetration testing without prior comprehensive vulnerability scanning as well as review of management and operational controls is not an effective method of assessing the security posture of a network, system or application.

4.10.3 Evaluating Vulnerability Scanning and Penetration Testing Results

The IV&V Analyst can assess the quality, completeness, and accuracy of the testing and Test Report by examining how the tester:

- Organized and consolidated similar vulnerabilities and provided the CVE or CAN (CVE Candidates) number for a vulnerability (if applicable)
- Defined and characterized external versus internal vulnerabilities and the system boundaries
- Categorized vulnerabilities into high, medium, and low risk vulnerabilities
- Provided multiple options for mitigating vulnerabilities
- Evaluated the raw data they collected and followed a documented process
- Eliminated false positives by correlation of data from multiple tools to identify and remove false positives and interacted with system administrator and other technical staff to eliminate false positives prior to presenting the Test Report

A Test Report that simply repackages the output of the scanning/assessment tool used should not be accepted and is an indication of poor analysis.

4.10.3.1 Introduction

The introduction section of the Test Report should provide background information appropriate to the evaluation and demonstrate an accurate understanding of the system or application including the mission of the Federal Student Aid organization, purpose of the scanning and/or penetration testing, and should have references to the ROE (if not referenced in another section of the Test Report).

4.10.3.2 Scope

The scope section of the Test Report should discuss the system boundaries associated with the assessment and provide the technical details of the assessment scope including the external and internal vulnerabilities the scanning and/or penetration testing is intended to identify.

4.10.3.3 Assumptions

The assumptions section of the Test Report should identify any assumptions and/or known preconditions associated with the scanning and/or penetration testing including requirement for access to networks and devices to be tested, availability of Federal Student Aid and/or contractor technical personnel to monitor testing, limitations of testing to discover vulnerabilities, and assumptions that accurate technical information is provided by the client. The assumptions may reference the ROE as appropriate for additional information.

4.10.3.4 Tailoring

The Test Report should address any unique needs or concerns of Federal Student Aid. The methodology, tool set, and rule set used to perform vulnerability scanning and/or penetration

testing should reflect Federal Student Aid input. The level to which the testing complied with Federal Student Aid requested methodology, tools, and scanning rule set use should be a major IV&V evaluation factor for the quality and completeness of the test.

Section 5. Independent Verification & Validation (IV&V) Reporting Standards and Procedures

5.1 Overview

These IV&V Reporting Standards and Procedures establish the reporting requirements necessary for the IV&V Team to fully document its activities for Federal Student Aid target systems throughout their development and implementation. Execution of a plan that follows these guidelines will help to ensure that the IV&V Team can consistently provide a common reporting format for all Federal Student Aid deliverables.

IV&V reporting will occur throughout the target LCM. The IV&V Team will document all IV&V results, which will constitute the specific report generated for each IV&V task. These IV&V reporting standards and procedures specify the content, format, and timing of all IV&V reports to be utilized for Federal Student Aid. These IV&V Standards and Procedures describe how results will be documented for implementing the IV&V Standards and Procedures described in Sections 2 and 3. All of the reports and checklists related to Security Effectiveness Evaluation are identified in Section 4.

The IV&V process results in the reporting products discussed in this section being delivered on a regular, timely basis to Federal Student Aid. This approach emphasizes building in quality up-front via a structured internal review process ensuring that each delivered product meets Federal Student Aid quality standards. The key objective of these standards and procedures is to provide Federal Student Aid with visibility into details of the development effort in a consistent format. For key deliverables, the actual plan and report templates are provided within these procedures. For other reports and memos only the recommended content is provided. In addition, different options are provided in the template based on what has been successfully used within Federal Student Aid. The IV&V Team will perform walkthroughs of all key deliverables before they are delivered to the Federal Student Aid Program Manager. Non-key deliverables will be reviewed by at least one other IV&V Team analyst as a quality review. The following procedures provide guidance for these activities.

5.1.1 Documentation Control

The IV&V Team will manage all documentation with the document files regularly reviewed and documents will be tracked by version. When it is necessary to keep multiple versions of a given document, the latest version will be marked accordingly and all of the latest document versions will be kept in the current files with the previous versions marked as archived. In addition, the IV&V Team will review all documents using the checklists included in Appendix C of the IV&V Standards and Procedures, and will maintain and track all document review comments.

Comments will be tracked by a unique sequential number assigned by the IV&V Team. When an updated document is released, the document will be reviewed for incorporation of all outstanding comments and dispositioned. All current IV&V procedures and plans will be kept on file and all personnel will be familiar with the contents.

The IV&V Team will prepare a file for each document to include the following:

- Master copy of document
- Notes (e.g., walkthrough dates)
- Completed Checklist (if applicable)
- IV&V Findings (e.g., comments, technical report)
- Comment Responses
- Correspondence with Federal Student Aid, developer, etc.

The IV&V Team will also maintain a document tracking log to include the following information:

- Document name
- Version and assigned tracking number
- Author of document
- Date received by IV&V Team
- Primary reviewer
- Internal comment walkthrough date
- Comment due date to Federal Student Aid/developer
- Actual comment delivery date
- Comment resolution and date

The IV&V Team will utilize this tracking system to create an overall Document Review Schedule. An example of a Document Tracking Log and Document Review Schedule is included in Appendix E. The specific comment and walkthrough process is described in Sections 5.1.2 and 5.2.2.5.

The IV&V Team will maintain a Deliverable file for each report provided to Federal Student Aid. This file will include the specific type of reporting template used for the IV&V activity, as well as a printout of the attached email to accompany each contract deliverable. The email will reference the specific attachments (e.g., Checklists), as well as the distribution of the deliverable.

5.1.2 Walkthroughs for Federal Student Aid Deliverables

The implementation of effective quality control is critical to the success of any major IV&V effort. The IV&V Team will review and monitor the IV&V reporting process, including contract data requirements list items and delivered products, to ensure that the items satisfy all applicable contract requirements. The IV&V Team will institute a strict deliverable quality procedure where every deliverable is reviewed by at least one additional senior engineer before it is released.

This section details the reporting guidelines and activities required to conduct a formal product walkthrough. The IV&V Team will utilize the following approach in preparation of Federal Student Aid contract deliverables:

- Plan and schedule the walkthrough

- Distribute the review materials
- Review the materials
- Conduct the walkthrough
- Document any defects and/or issues
- Resolve and verify the resolution of the defects and/or issues
- File the review materials

5.1.2.1 Planning the Walkthrough

The IV&V Team will schedule the internal walkthrough and prepare the required forms. The distribution of review materials must be provided early enough to ensure that there is adequate review time for the meeting participants.

5.1.2.2 Preparing the Meeting Notice

The IV&V Team moderator will prepare the Walkthrough Meeting Notice template by filling in:

- Block #1 – Product/IV&V Control Number
- Block #2 – Author(s)
- Block #3 – Walkthrough Number, Date, Time, and Place
- Block #4 – Reason for Walkthrough
- Block #5 – Review Team, Moderator

If the walkthrough is a follow-on to a previous walkthrough whose disposition was "Not Accepted," the previous walkthrough will be cross-referenced in Block #4. A sample meeting notice is provided in Appendix E.

The Walkthrough Log will be used to record details of the walkthrough and obtain the next consecutive walkthrough number. The IV&V Team will complete the following items when planning the walkthrough:

- Column 1 – Walkthrough Number
- Column 2 – Product
- Column 3 – Author
- Column 4 – Moderator
- Column 5 – Walkthrough

A sample walkthrough log is provided in Appendix E.

5.1.2.3 Distributing Review Materials

The completed Walkthrough Meeting Notice, the materials to be reviewed, and any supporting information will be copied and distributed to the moderator and reviewers. The moderator will receive copies of the Defect/Issue List to document defects or issues found during the walkthrough. The Defect/Issue List contains: the issue number, the defect/issue category (critical, minor, issue), the resolution (resolved, verified) and the comments. A sample defect issue list is provided in Appendix E. Any supporting documentation or other data that is

included in the walkthrough package should be marked “for your information” (FYI), to distinguish it from the other material under review.

5.1.2.4 Reviewing the Materials

Materials distributed for the walkthrough will be reviewed by the participants prior to the meeting. Participants will arrange for a substitute reviewer or forward their review comments to the moderator prior to the walkthrough if they are unable to attend.

5.1.2.5 Performing the Walkthrough

The moderator will document walkthrough attendance on the Walkthrough Meeting Notice (Block #6) by recording the attendees’ names or by use of a note indicating who did not attend. The moderator will also fill out the header information on the Defect/Issue List. If a majority is not present or the reviewers are unprepared, the moderator will reschedule the walkthrough and the meeting will be adjourned.

If a majority is present and the reviewers are prepared, the moderator will begin the meeting by introducing the product under review, and then give a brief introduction of the walkthrough materials. Next, the moderator will proceed by stepping through the walkthrough materials (i.e., page by page, diagram by diagram, module by module, etc.) with the participants commenting on areas of concern. The moderator will also interject the comments of any reviewers not able to attend. The moderator will ensure that: all decisions are made by the team; no one person dominates; feedback is provided for self-evaluation; and changes agreed to are documented.

If an issue or defect is found, the moderator will record it on the Defect/Issue List. Each defect or issue will be tracked by a unique number and identified as based on the following categories:

- Comment requires immediate resolution.
- Comment requires resolution to meet exit criteria.
- Design quality or style suggestion.
- Question about the document.
- Comment has been resolved with developer.
- Comment discussed with developer/still open.
- Recommendation for future improvement.
- Typo, spelling, or minor wording changes.

An alternative to logging each defect on the Defect/Issue List will be to redline the original review materials. When redlines are used, at least one defect/issue description will be logged for each separate document or unit (example comments: "see redlined master" or "see redlines").

The same walkthrough may be continued over more than one meeting by giving it a disposition of "Not Completed" and providing rationale. When all materials have been reviewed, the review team will agree upon the disposition of the walkthrough based upon the defects/issues recorded during the walkthrough. (See Appendix E for sample).

5.1.2.6 Resolving Defects/Issues

Critical defects have significant impact and their resolution requires a repetition of the walkthrough for those portions of the product affected. When the revision is complete, the moderator will schedule a new walkthrough.

The IV&V Team will resolve all minor defects and issues by incorporating solutions identified during the walkthrough. The Defect/Issue List will be completed to describe the resolution of each issue. The moderator will indicate that the defect or issue has been corrected by initialing the resolution field. The moderator will deliver the original review materials, Walkthrough Meeting Notice, Defect/Issue List, and the updated version of the materials to the IV&V Team for verification.

5.1.2.7 Verifying Defect/Issue Resolution

The moderator will verify that all minor defects have been corrected and all issues addressed, and will indicate compliance by initialing the Defect/Issue List. When redlines are used, the moderator will place a check mark by each redline to indicate that the item has been addressed. If there are defects which have not yet been resolved, or issues that need to be addressed, the moderator will return the materials to the author of the report for correction. This iterative cycle will continue until the moderator is satisfied that all necessary changes have been made to the review materials.

5.1.2.8 Completing the Walkthrough

Hours expended for a walkthrough may be calculated by summing all reviewers' preparation time, hours expended in walkthrough meetings, and the time spent by the moderator in resolution verification. This optional data will be entered in Block #8 of the Walkthrough Meeting Notice. The moderator will close a walkthrough by signing and dating Blocks #9 and #10, and returning the review materials to the author of the report.

5.1.2.9 Filing the Walkthrough Materials

Each completed walkthrough will be filed (paper or electronic) and will contain a copy of:

- The Walkthrough Meeting Notice
- Defect/Issue List
- All redlined review materials
- The final version of the product

5.2 IV&V Reporting Standards and Procedures

The following paragraphs describe the IV&V reporting standards and procedures, which include reporting requirements and timeframes necessary to provide to Federal Student Aid the results of the IV&V Team's efforts. The IV&V Team will thoroughly document all IV&V efforts and inform the Federal Student Aid Program Office of their findings as the tasks are performed. Evaluations, comments, audit reports and white papers related to IV&V activities will be generated by the IV&V Team and communicated to the developer through the Federal Student Aid Program Office. The IV&V Team will utilize checklists to monitor task performance and product delivery. Examples of the types of checklists that may be used are included in Appendix

C of this IV&V Handbook. The IV&V Program Manager will closely monitor the accuracy and quality of all deliverables and IV&V results.

5.2.1 Reporting Overview

The IV&V Team will have a standard for the time required to review documents as well as to respond to comments. This time will be a function of the type of document (e.g., requirements, design, and test) as well as the number of pages in the document, but is limited to no more than four weeks. However, as for major reviews, the IV&V Team may submit “quick look” comments as necessary. The IV&V Team will generate a “quick look” comment package that identifies significant issues that must be addressed at major reviews. In the four weeks following the review, the IV&V Team will perform a “full up” review and submit a coordinated comment package to the developer. These comments will be adjudicated over the next several months.

5.2.2 Reporting Templates

The IV&V reporting requirements are shown in Exhibit 5-1. The IV&V Team will utilize the reporting templates and matrices, along with the associated procedures to implement them, as described in the following paragraphs. These standards necessitate the use of reporting templates which are included within the text for readability, and templates are included in Appendix E for ease of use by the IV&V Team. Each template will be available in an electronic format for use by the IV&V Team. These templates should be used as guidelines for preparing plans and reports. Some of these will be tailored based on the needs of the Federal Student Aid organization sponsoring the review. However, the data elements in these templates represent the information traditionally required for these reports.

5.2.2.1 IV&V Plan

The IV&V Team will prepare a tailored plan to address the IV&V activities for each target system under review. This will follow the IV&V Standards and Procedures and/or any other applicable guidance documents. This plan will be fairly brief and contain an introduction and a list of activities to be performed for each development stage. The tailoring will be based on the unique aspects of the target system but must follow Federal Student Aid standards. The plan should be structured by phase and include key activities for each phase with target due dates.

Exhibit 5- 1, IV&V Reporting Requirements

IV&V REPORT	STAGES					
	Vision	Definition	Construction & Validation	Implementation	Support & Improvement	Retirement
IV&V Plan	•	•				
Completed Checklists	•	•	•	•	•	•
Technical Reports	•	•	•	•	•	•

IV&V REPORT	STAGES					
	Vision	Definition	Construction & Validation	Implementation	Support & Improvement	Retirement
Document Review Comments	•	•	•	•	•	•
Memorandum of Record	•	•	•	•	•	•
Review Plan		•	•	•	•	
Review Report		•	•	•	•	
Feasibility Assessment Report	•					
Requirements Verification Matrix		•	•	•	•	
Anomaly Report			•		•	
Risk Watch List	•	•	•	•	•	•
IV&V Test Procedures and Use Cases			•	•		
Test Report			•	•		
Special Studies Report	•	•	•	•	•	•
PRR Recommendation			•			
IV&V End of Phase Summary Report	•	•	•	•		
IV&V Final Report				•		
Progress Report	•	•	•	•	•	•
Trip Report	•	•	•	•	•	•
Issue Log	•	•	•	•	•	•
IV&V Metrics Report	•	•	•	•	•	•

The IV&V Plan will describe the following:

- Target system profile
- IV&V schedule
- IV&V Team organization
- Scope of the IV&V effort (Approach, Activities, Tailoring)
- Points of contact
- Key activities by phase
- Key deliverable due dates
- Tailoring of IV&V tasks and/or checklists based on project and/or scope

The IV&V schedule will be coordinated with the developer’s project master schedule, and will be submitted in a Federal Student Aid-specified format/medium so that IV&V schedules can be consolidated across all IV&V contractors. The IV&V Plan will be submitted no later than 30 days after the authorization to proceed.

5.2.2.2 Review Plan

Reviews will be performed when scheduled by the IV&V Team or when directed by Federal Student Aid. The lead reviewer will determine when to begin planning a scheduled review. Planning will also begin when a client requests or directs that a review be performed. The IV&V Team will provide the Review Plan for review within 10 days of the scheduled review. Review personnel will be restricted to individuals who did not develop the product or perform the activity being evaluated and must not be responsible for either the product or the activity being evaluated. The lead reviewer and the client will agree on the details of the evaluation such as:

- The scope of the review and time frame for performing the review activities, including the beginning and ending date(s)
- Knowledgeable points of contact within the audited organization who will be accessible during the review
- Any resources required
- Sources for the criteria to be applied to the products or activities being evaluated

The review client is the individual who requested or directed that the review be performed or who has a direct interest in the findings. The lead reviewer will be responsible for preparing the Review Plan. A sample review plan is included in Appendix E. Data will be entered into the Review Plan as follows:

Exhibit 5- 2, Review Plan

Area	Description
[Block #1]	State the audit subject and objective.
[Block #2]	Fill in the project name (e.g., Portals, IFAP).
[Block #3]	Date the audit plan was prepared.
[Block #4]	The lead auditor is the "preparer."
[Block #5]	The Federal Student Aid Program Manager, or designee, is the "reviewer" and must approve the audit plan.
[Block #6]	Enter the "client's" name leaving room for their approval.
[Block #7]	This can be any organizational descriptor that identifies an activity or product or may be a Computer Software Configuration Item.
[Block #8]	Date(s) scheduled for the audit. An audit may cover a period between program milestones (e.g., Critical Design Review to Test Readiness Review).
[Block #9]	Identify the lead auditor and fill in the names of the other auditors.
[Block #10]	Enter the designated points of contact in the audited organization.
[Block #11]	List resource requirements of which the reviewee must be aware, such as required access to personnel, equipment, passwords, or reports.
[Block #12]	List the documentation from which the audit criteria are drawn. Sources often include the Software Development Plan, software procedures, and program manuals.

Area	Description
[Block #13]	Audit instructions contain the details of how the audit will be conducted, beginning with a statement of the purpose and specifying what will be examined and the criteria to be used. For all audit activities, describe the audit method through which adherence to the requirements is determined and include specifics, such as sample size. Review criteria will be specified for each element being evaluated. Instructions will be written in sufficient detail to allow another member of the IV&V Team to conduct the audit if needed.

The Review Plan will be reviewed and approved by the Federal Student Aid Program Manager. Next, the client will review and approve the Review Plan. Upon approval, both signers will receive a copy. The lead reviewer will also provide a copy of the approved plan to the reviewed organization in advance of the review.

Attachments (i.e., checklists or data recording sheets) may be prepared and used to support review execution and will be appended to the Review Plan. Checklists will be used when conducting interviews to ensure that the same questions are asked of each person. The IV&V Team will maintain standard checklists which may be modified for some reviews. Data recording sheets may range from informal handwritten notes to tailored forms.

The Review Plan may be used in lieu of a checklist if it contains more product and/or process criteria than would be contained in a standard checklist.

5.2.2.3 Completed Checklists

The IV&V Team will complete the appropriate checklist (as described in Sections 3 and 4) for each IV&V task. Completed checklists may be included as part of a Technical Report submitted for the specific IV&V task. Sample checklists are included in Appendices C through E of this IV&V Handbook.

5.2.2.4 Technical Reports

The IV&V Team will report on the individual IV&V phase tasks in a letter of findings (technical report) which will be issued as necessary. The technical reports may document interim results and status. The reports may be in a format appropriate for technical disclosure (for example, technical reports or memos). Reports will be generated for each technical task performed during the course of the IV&V program. Specific IV&V tasks are defined in Section 2.3. Security assessment tasks are defined in Section 4. Technical reports will be due no later than 30 days after completion of each reportable activity (for example, audits and product reviews).

Technical reports will be utilized to report on all formal concept, requirements, and design reviews. Technical reports will be utilized to report on test readiness reviews by providing recommendations relative to the start of testing. The IV&V Team will also provide a technical report relating to Production (Operational) Readiness Review and Post Implementation Review.

In general, the technical reports will:

- List the evaluation participants and objective(s)
- Document detailed results and findings
- Detail the extent, cause, impacts, and frequency of any problems or negative trends detected

- Provide appropriate corrective action and/or preventive measure recommendations

5.2.2.5 Document Review Comments

The IV&V Team will prepare and submit document review comments in a letter of findings. For each document that requires review, the IV&V Team will submit a letter of findings within 30 days of document receipt. When dictated by schedule, “quick look” reviews will be performed to informally provide key comments as early as possible.

The process of document (or “product”) inspection helps ensure that products of processes meet Federal Student Aid requirements and that intended audiences obtain a quality perspective of those processes. Document inspections will be conducted in a systematic manner, beginning with the receipt of each document into the inspection (or review) process, continuing through the generation and coordination (among other IV&V Team personnel) of informal and formal comments and recommendations, and culminating in the verification of adequate disposition of these comments or recommendations. Checklists serve to normalize subjective evaluation by multiple reviewers.

Following an established order of inspection, coordination, and verification (as described in Section 3.2.1) will result in more thorough and efficient reviews of Federal Student Aid documents and will provide an effective feedback mechanism regarding the evolution of, and insight into, the development, implementation, and deployment of the Federal Student Aid target system. As discussed in Section 5.1.1, the IV&V Team will track completion and delivery dates for documents in accordance with schedules published by the Federal Student Aid program office. The IV&V Team representatives will use these schedules to allocate time for inspection of system documents so that the necessary time to complete an inspection can be reflected in the IV&V Team schedule. The IV&V Team reviews will be completed and comments provided in a timely manner to support effective feedback.

The IV&V Team will use applicable government specifications and internally generated checklists to conduct document inspections. Checklists for content are tailored from the IV&V Standards and Procedures, while document style and format are checked against applicable pertinent sources, such as Federal Student Aid procedures. Checklists will be tailored in accordance with any guidance provided by the program office or as directed by cover letters or memos accompanying the document to be inspected.

To begin the document inspection process, the IV&V Team will obtain a blank comment form and provide any tailoring for the specific document. A template is provided in Appendix E. Comments will be provided in the following table format to facilitate a quick turnaround time for providing comments to Federal Student Aid. A MOR (discussed in Section 5.2.2.6) can also be used for distributing comments. Comments will provide the page number where the comment applies, including the section, figure or table. The comment text must provide enough information to stand alone without previous knowledge or additional information. Comment text will consist of the identification of any deficiencies in correctness, consistency, completeness, accuracy, and readability, as well as provide recommendations for corrections and/or improvements. Categories are provided to offer additional information as to the criticality of the comments, as well as the nature of the comments.

If necessary, comments may be provided one per page to ease delivery to appropriate individuals. The table itself may be electronically mailed, and the e-mail should contain the document name and date, as well as a brief summary of the findings.

5.2.2.6 Memorandum of Record (MOR)

The MOR is a formal memo format that can be used for meeting minutes, comments, and status reports, or to highlight a significant issue or milestone. It is easily tailored and provides a means of highlighting any concerns or issues that need to be brought to the attention of Federal Student Aid Management. The memoranda are divided by type including customer satisfaction, design review, inspection/test results, process action team, and other IV&V/QA.

5.2.2.7 Review Report

After completion of a review, the IV&V Team will prepare a report. The report will be distributed within 10 days of audit completion. A copy will be filed with the associated Review Plan and any supporting materials that were gathered during the audit. The Federal Student Aid Program Manager will approve the Review Report prior to its distribution.

Information should be entered into the Review Report template as follows:

Exhibit 5- 3, Review Report

Area	Description
[Block #1]	Actual date(s) of the review
[Block #2]	Identify the lead reviewer and fill in the names of the other auditors.
[Block #3 - Optional]	The total effort expended on the review may be broken out by planning and preparation time, review performance, and reporting. Time to prepare the preliminary review findings and conduct the debriefing may be included in the review time.
[Block #4]	The narrative will include: the scope of the audit, the execution date(s), and a highlight of at least one significant finding. If there are no findings, that should be stated. Include a general statement describing the developer's performance improvement or decline since the previous review. It is also appropriate to comment on well executed processes or outstanding products.
[Block #5]	Number each finding. A finding document a discrepancy discovered during the current review, or a previous one, and is classified as either major or minor. Findings cite, by reference, the requirement not being met, its severity compared to the results expected, and an explanation. A finding may be related to a failure in the process or to a failure to execute a plan or process, but the auditor does not attempt to make this determination. The cause will be determined during the corrective action process. Corrective actions will be referenced with the appropriate finding.
[Block #6 - Optional]	This block will include items of interest and/or observations made during the review that do not qualify as a finding.
[Block #7]	The reviewers sign the original report prior to its distribution.

5.2.2.8 Feasibility Assessment Report

The IV&V Team may, at the option of the Federal Student Aid Program Manager, prepare an independent Feasibility Assessment Report. This report will contain a detailed analysis of the IV&V Team's assessment of the alternatives including:

- Assessment methodology

- Alternatives with accompanying analysis
- Ranking of alternatives
- Recommendations with rationale
- Any risks that accompany the recommendations and alternatives

The Feasibility Assessment Report will be submitted within 30 days of Federal Student Aid request.

5.2.2.9 Requirements Verification Matrix (RVM)

The IV&V Team will prepare a Requirements Verification Matrix (RVM), as a tool to verify that system requirements are in accordance with the IV&V standards outlined in Section 2. The RVM consists of the independent requirements database and a series of columns used to record traceability from requirements to design to software component to test case. The appropriate column(s) are added to the RVM as the development progresses from one phase to the next. The RVM will be in a spreadsheet or database format capable of producing the report provided in Appendix E.

5.2.2.10 Anomaly Report

An Anomaly Report will be prepared and submitted to the Federal Student Aid Program Manager for anomalies detected by the IV&V team. Anomaly Reports will be provided to Federal Student Aid and the developer no later than 3 days after anomaly detection. Each Anomaly Report will contain the following information:

- Description and location
- Impact
- Cause (if known)
- Criticality
- Recommendations

The IV&V Team will perform statistical and qualitative analyses on any target system anomalies to identify and analyze trends indicative of systematic problems. Because the inception-to-implementation lifecycle may span several months, the IV&V Team will track the current status of system problems and deficiencies to assure the validity of any resultant changes. Anomalies will be categorized as to criticality and reported informally as part of the reviews and Integrated Product Teams and formally as part of the status reports and deliverables. The IV&V Team may review corrective actions, verify priorities, and confirm the disposition of the change. The IV&V Team will utilize the Incident Report form provided in the Federal Student Aid System Integration and Testing Approach document for consistency with the developer. A copy of this template is provided in Appendix E.

5.2.2.11 Risk Assessment Report and Risk Watch List

The IV&V Team will provide a formal report documenting the results of the risk assessment described in the IV&V Standards and Procedures. This memorandum will contain a description of the risk assessment methodology, a description of the rankings, and a report of each risk with a recommended mitigation strategy. The risk assessment will be due no later than 10 days after completion of the assessment.

A Risk Watch List will be generated from the risk assessment and will be reviewed with the Development Program Managers. The Risk Watch List will be delivered bi-weekly and should be continually monitored by the IV&V Team. A detailed discussion of the risk management process and a sample Risk Watch List are included in Appendix D.

5.2.2.12 IV&V Test Procedures and Use Cases

The IV&V Team may prepare independent test suites that will include:

- The title of the test case
- Purpose
- Test Environment (specific setup needed for test)
- The analysis required of the results, if applicable
- Step-by-step instructions with expected results and requirement being satisfied

These procedures and use cases will be provided sequentially throughout the Build and Test and Integration Test Phases in preparation for Acceptance Testing. A sample test procedure/use case is included in Appendix E.

5.2.2.13 Test Report

The IV&V Team will monitor formal testing and submit reports within 15 days of each test completion. These reports will be used to document the IV&V Team's witnessing of test activities including software installation, test setup, test execution, problem reporting, data recording, and data analysis.

As directed, the IV&V Team will witness developer testing for the purpose of verifying that the documented plans and procedures are executed properly and that the designated requirements were adequately tested. The IV&V Team will also analyze the objective evidence provided by the developer's test results. A Test Report may be prepared by the IV&V Team upon completion of the entire test activity. The report will contain an executive summary, overview of the test activity, a table showing the disposition of the requirements, a summary of the requirements testing results, and an optional section containing any lessons learned with recommendations. The report may contain the IV&V Team's recommendations that were provided during the test effort including the recommendation as to whether or not to proceed with the testing. During periods of compressed schedule, test results may be reported in the IV&V End of Phase Summary Report or the IV&V Final Report.

Following independent test execution, the IV&V Team will prepare an IV&V Test Report documenting the independent test results. The IV&V Test Report will be submitted within 15 days of test completion.

The following Test Report data will be included, at a minimum. A template is included in Appendix E.

Executive Summary - A short, high-level synopsis of the test activity; include the location(s), relevant dates, major groups who participated, and an overall conclusion of how successful the testing was in meeting the overall objectives.

Test Activities - Describe the results of the preparation activity; provide an overview of the test activity; and include a statement summarizing the results obtained.

Requirements Table - A table that shows the disposition of the requirements. This table uses functional area which is dependent upon the actual test activity and the specific requirements that are to be validated.

Test Analysis - Summarize the results of the requirements testing; any significant problems encountered and their cause(s), if known; solutions which were incorporated; action plans agreed to; proposed recommendations; an overall conclusion on the level of accomplishment of the core test objectives; and any additional observations on how the testing was conducted.

Lessons Learned - This section of the report may include both positive and negative lessons learned during the test effort. Positive lessons learned will be written in enough detail to provide a clear understanding of the immediate and the long term benefits realized by the program and also clearly describe how this was achieved so it will be easily understood and adopted for future use. For problems encountered, include a statement of the deficiency; cause, if determined; action(s) taken or planned; and a recommendation to prevent future occurrences.

5.2.2.14 Special Studies Report

As required, the IV&V Team will conduct and report on technical, cost, and schedule trade-off analyses related to system development (for example, changes in standards or technology). These efforts are specifically identified and approved by Federal Student Aid prior to commencement. This may take the form of a formal memorandum or be done using the Special Studies Report Template in Appendix E. The study will describe the purpose, how it was performed (Approach), findings, and summary of results. The results of the study will be provided within 10 days after its completion. The report will document technical results and will include, at a minimum, the following information:

- Purpose and objectives
- Approach
- Findings
- Summary of results

5.2.2.15 IV&V End of Phase Summary Report

For large system development efforts, the IV&V Team may prepare and submit an IV&V End of Phase Summary Report for each lifecycle phase to include the following information:

- Description of IV&V tasks performed
- Assessment of overall system/software quality
- Recommendations to proceed to next phase
- Lessons learned

The End of Phase Summary Report is a living document which will identify all activities performed by the IV&V Team during the phase just completed. The document will be issued each time a developer completes a phase. The previously published information will be updated and the risk area will be reassessed. An update summary of the previous phase will be provided

when the subsequent summary report is issued. A template for the End of Phase Report is included in Appendix E.

An End of Phase Summary Report will be provided at the conclusion of each of the following phases:

- Vision Phase
- Definition Phase
- Construction Phase
- Deployment Phase
- Support Phase

For the Deployment Phase, this report will be the IV&V Final Report. Support phase activities will be reported using Memorandum of Record and comment forms. The End of Phase Summary Report will be formally structured and include the following elements:

Executive Summary - This paragraph will provide a brief statement of the IV&V Team activity results from the previous phases. An overview of the activities for this phase, a summary of the results of this phase, and an evaluation of phase completion will be provided.

Introduction - This section will identify the target system (e.g., Federal Student Aid system name) and the phase just completed where this report applies. It will include the purpose, scope, and expected results of this report on the program. The scope will identify the specific topics to be covered in the report, and any exclusions will be specifically identified.

Phase Activities and Assessments - This section will be divided into paragraphs to identify each activity performed by the IV&V Team relating to the identified system during this phase, methodology used in the performance of the identified activities, a summary of results for each activity, and any recommendations that are related to issues that have not been resolved satisfactorily during the phase. All recommendations must provide a rationale.

Overall Phase Assessment - This section will provide an overall assessment of the system. These overall assessments will include overall anomalies and resolutions, system metrics and risks to the program.

Conclusions and Recommendations - This section will provide an overall statement of Federal Student Aid system status. Overall conclusions drawn for the phase will be provided along with lessons learned. Any recommendations for corrective action or improvement will be justified.

Lessons Learned - This section will provide lessons learned during the development phase.

5.2.2.16 Production Readiness Review Recommendation

IV&V should encourage a Pre-Production Readiness Review where all outstanding issues can be addressed prior to PRR. A sample template is included in Appendix E. At least one full day

prior to PRR, IV&V must provide the Enterprise Quality Assurance Manager a Technical Report or email which includes the following:

- List of outstanding issues
- Risks relevant to PRR
- Recommendation for PRR
- All contingencies that impact the recommendation
- The IV&V Project Manager or team lead must sign the PRR recommendation.

5.2.2.17 IV&V Final Report

The IV&V Final Report will be issued at the end of the System Deployment Phase or at the conclusion of the IV&V effort. The IV&V Team will prepare and submit a final report addressing the following items:

- Summary of all lifecycle IV&V tasks
- Assessment of overall system quality
- Recommendations
- Lessons learned

This formal report will follow almost the same format as the End of Phase report, the major difference being that the Final Report will discuss issues from the entire development lifecycle, while the End of Phase report specifically addresses one phase of the development effort. The Lessons Learned will also be provided in the Federal Student Aid MS Word Template.

5.2.2.18 Progress Report

The IV&V Team will provide a summary of all IV&V activities performed for the program. The IV&V Team lead will compile IV&V Team personnel status information and generate a report. This report will summarize all IV&V activities for the target system, including both formal and informal deliverables. This report should be tailored for the IV&V effort and may also take the form of weekly status reports (see Appendix E for sample). The report will include:

- Accomplishments for this period
- Scheduled Tasks for next period
- Meetings for the previous week and upcoming meetings
- Recommended Federal Student Aid actions
- Preliminary issues
- Issue log of outstanding issues for monitoring purposes

The issue log is a means of capturing and tracking all issues reported in the weekly status report. Rather than reporting the same issues on a weekly basis, the IV&V team will keep a cumulative log of all outstanding issues and review them with the development team. Priority should match the developer definitions for each project for consistency. Typically, priority one is a critical issue, two is a medium range concern, and three is a minor issue. This can be tailored for the project. Status would be open or closed, and resolution should state why it was closed.

A template for this and other status reports is included in Appendix E. If a monthly report is preferred by the QA lead, the following sections must be included:

Section One - The IV&V Team Executive Summary section provides a summary of IV&V activities and will be no longer than one page. A paragraph at the end of the summary outlines key activities planned for the next month.

Section Two - The Deliverables section provides a table of all the deliverables made during the month under review (separate table for each contract line item number (CLIN)). For multiple CLINs or task orders, a separate table can be prepared for each, or a column can be added identifying the task number. This section also includes meeting and phonecon dates for the reported month.

This section will also address any concerns, outstanding issues, or risks to the program identified by the IV&V Team.

5.2.2.19 Trip Report

The IV&V Team may prepare and submit formal trip reports to the Federal Student Aid Program Manager for each trip in support of Federal Student Aid. Trip Reports will be due no later than 10 days after return from the scheduled trip. These reports may be in the form of informal memoranda or can be delivered via electronic mail and then followed up with a formal delivery. A template is included in Appendix C. Trip Reports may be unnecessary if a report is already part of the outcome of the trip, e.g., Site Visit Report, etc. A Trip Report memo must contain:

- Purpose of trip
- Location of trip
- Dates of travel
- Personnel traveling
- Summary
- Findings
- Actions/Issues
- Lessons learned (if applicable)

5.2.2.20 IV&V Metrics Report

The following is the outline of IV&V Metrics Report, used in reporting metrics performance on a monthly basis. A more detailed description of the metrics reporting is discussed in Section 6.3.2. (The template for this report is included in Appendix E):

1.0 Introduction

1.1 Methodology

1.2 Summary of IV&V Accomplishments

1.2.1 Ongoing Activities

1.2.2 New Activities

2.0 Assessed [Reporting Month] Deliverables

3.0 All defects are reported by LCM stage in the lifecycle. Defect Categories (for consistency, all assigned metric values with a “1” represent a **major** impact or discrepancy, a “2” represents a **moderate** impact or discrepancy, and a “3” represents a **minor** impact or discrepancy

4.0 Issues and Findings Count (by breaking down the [*reporting month*] metric numbers into major impact / deficiency (assigned metric value of “1”), moderate impact / deficiency (assigned metric value of “2”), and minor impact / deficiency (assigned metric value of “3”), the appropriate percentages can be derived.

Breaking down the [*Reporting Month*] metric numbers into major impact / deficiency (assigned metric value of “1”), moderate impact / deficiency (assigned metric value of “2”), and minor impact / deficiency (assigned metric value of “3”), the following percentages were derived:

	Total	Percentage
Major impact / deficiency:		
Moderate impact / deficiency:		
Minor impact / deficiency:		
TOTALS		

5.2.2.21 Funds Expended Report

The Funds Expended Report is a Microsoft Excel Template that provides the Enterprise Quality Assurance Manager and Team Leads with an analysis of the IV&V budget including the total budget, funds expended, and the remaining funds. It is provided on a monthly basis.

5.2.2.22 Contractor Team/Security Roster

The Contract Team Roster, also known as the Security Roster, is delivered at the project inception and includes a list of the complete project staff including name, labor category, task, title, clearance status, whether they have a badge, and whether they are on or offsite. This roster should be updated whenever a change is made to the project team.

5.2.2.23 Executive Level Project Report

This report provides Federal Student Aid’s leadership insight into the key issues facing a particular development project. This report gives IV&V’s formal assessment of the issues and provides a forum for IV&V to convey information to senior management.

- A red light indicates a critical issue that will impact the ability to complete the project. Management must take action to address this issue and it should be given the highest priority.
- A yellow light is a medium range concern that should provide a warning to management that this area should be watched and possibly more oversight is required.
- A green light indicates that there are no significant issues and the project is on track.

It is important that IV&V include development managers in this process so that they are not “surprised” by any data in this report. While it is important to make sure the development

managers are included, this report must reflect IV&V's independent analysis of the project, even if that analysis differs from that of Federal Student Aid's development project manager. This report is submitted on a monthly basis throughout the life of the project and may be combined with the monthly report, at the discretion of Federal Student Aid.

5.2.2.24 IV&V Lessons Learned

At the conclusion of each IPR, IV&V will provide lessons learned for the quarter under review. The lessons learned will be entered into the Microsoft Word Template. This template includes relevant project data and a series of fields for each lesson including lesson title, background, description, source and category. The lessons learned should be submitted to John Olumoya.

5.3 Security Reporting Standards and Procedures

The format, content and templates for reports to be prepared in support of Section 4, Security Effectiveness Evaluations, are contained in the body of Section 4, and the appropriate Appendices referenced in that section. These functions are separate from traditional IV&V and have their own reporting mechanisms.

Section 6. Independent Verification & Validation (IV&V) Performance Standards and Procedures

6.1 Overview

The IV&V and Security Assessment Performance Standards and Procedures establish the performance measurement system and associated requirements necessary for the IV&V Team to document its activities in a measurable format for Federal Student Aid. Execution of a plan that follows these guidelines will help to ensure that the IV&V Team can consistently provide timely performance information in addition to a common performance measurement format to Federal Student Aid. IV&V and Security Assessment performance monitoring and measurement will occur throughout the target system development lifecycle. These IV&V and Security Assessment performance standards and procedures specify the content, format, and timing of IV&V and Security Assessment performance reports to be utilized for the Federal Student Aid Modernization Program. These standards and procedures are intended for Federal Student Aid to evaluate the IV&V or Security Assessment contractor and maintain a repository of performance information. These IV&V and Security Assessment performance standards and procedures allow for quarterly evaluation/review by Federal Student Aid.

6.1.1 Objectives

The goal of a performance measurement system is to ensure that the system is not too costly, produces high-quality data, and provides useful information for management and policy purposes. It should also enable the Program Manager to judge whether continuous improvement is being made in terms of efficiency and effectiveness, and to ensure that reported improvement in one of these areas has not been made to the detriment of another.

Performance measurement will provide assistance to Federal Student Aid IV&V and Security Assessment in:

- Performance Based Organization (PBO) tasks
- Coordination of multiple contracts
- Coordination of multiple projects
- Improvement in Federal Student Aid software development, IV&V, Security Assessment, and test processes
- System development status information distribution/dissemination
- Project risk management
- IV&V Metrics

Performance measures should be derived directly from the IV&V or Security Assessment program's goals and objectives. They should measure the extent to which specific goals and/or objectives are being accomplished. As a result, performance management contributes to better decision-making and accountability. It is important to examine program effectiveness or outcomes, rather than just quantity or efficiency.

A well-developed performance measurement system will enable the IV&V and Security Assessment Teams to spot weaknesses, as well as strengths and opportunities. Thus, better knowledge of strengths and weaknesses will give the Program Manager (as well as other users) an opportunity to diagnose IV&V and Security Assessment organizational growth capabilities and take relevant actions.

6.1.2 Performance Assessment

Performance measurement is the ongoing monitoring and reporting of program accomplishments, particularly progress towards pre-established goals. Performance measures may address the type or level of program activities conducted, the direct products and services delivered by a program, and/or the results of those products and services. A program may be any activity, project, function, or policy that has an identifiable purpose or set of objectives. In providing performance measures, the IV&V and Security Assessment Teams will use both metrics and assessment schemes such as peer review and customer satisfaction. Performance measurement will be constructed to encourage improvement, effectiveness, efficiency, and appropriate levels of internal controls. It will incorporate best practices related to the performance being measured and cost/risk/benefit analysis, where appropriate. Performance metrics will lead to a quantitative assessment of gains in customer satisfaction, organizational performance, and workforce excellence. The key elements of the performance metrics will address alignment with organizational mission, quality of product, timely delivery, cost reduction and/or avoidance (if applicable), cycle time reduction, customer satisfaction, meeting Department of Education requirements and meeting commitments.

The cause-effect relationship between IV&V or Security Assessment outputs and their eventual outcomes is complex. It will often be difficult to quantify these relationships empirically, even though obvious logical relationships exist between the outputs and outcomes. The difficulties may arise from:

- The long time delays that often occur between the IV&V and Security Assessment results and their eventual impacts
- The fact that a specific outcome is usually the result of many factors, not just a particular IV&V or Security Assessment program or project
- The fact that a single IV&V or Security Assessment output may have several outcomes, often unforeseen, rather than a single unique outcome
- Potential negative outcomes that can be prevented due to proactive IV&V or Security Assessment solutions

Consequently, the cause-effect relationship between IV&V or Security Assessment outputs and their resultant outcomes should be described in terms of logical causality. Quantitative empirical demonstrations should not be required, and are often not even possible. Customer satisfaction evaluations are a valuable tool for hard to measure outcomes. Since IV&V and Security Assessment outcomes are often not quantifiable, IV&V and Security Assessment measures should always be accompanied by narrative in order to provide full opportunity for explanation, presentation of evidence of success, and discussion of the nature of non-metric peer review and customer evaluation measures. Excessive tracking of metrics should be avoided when experience determines that they are not useful. Although it is important to be consistent in the

types of metrics and goals that are tracked, flexibility in dropping or adding metrics could prove very beneficial in arriving at the most useful set of metrics. Therefore, it is recommended that a set of mandatory measures, as well as a set of program-dependent measures, be designed and implemented for the specific IV&V or Security Assessment project. The entire set of performance measures will be described in the project-specific IV&V Plan discussed in Section 5.2.2.1.

6.2 IV&V Performance Standards and Procedures

Developing a performance measurement system involves an understanding of what the program is trying to accomplish and who the main users/customers are, as well as a basic knowledge of the level of service currently being provided by the program. The specific steps in the process are listed below:

- Identification of the program's critical success factors
- Selection of program-dependent performance measures
- Design of the collection and analysis process
- Monitoring
- Performance reporting
- Analysis and action

When designing a performance measurement system, the IV&V or Security Assessment Team will address the following issues:

- What are the uses for and who are the users of the data? Performance measurement reporting can be used for decision-making, performance appraisal, accountability, and improvement in performance.
- Which critical system success factors are related to IV&V or Security Assessment performance factors?
- What indicators should be candidates for reporting? To what extent are these indicators measurable, valid, and comprehensive?
- How and to what extent should indicators be disaggregated? There is no standard approach to disaggregation of performance; it is commonly categorized by degree of difficulty of the incoming workload, or type of service.
- What comparison information should be reported for the various indicators? Comparisons can be made between current information and previous performance, similar jurisdictions, technically developed standards, actual goals set by the agency, etc.
- What explanatory data should be included along with the performance data, and how should it be presented?
- To what extent are the indicators verifiable? Performance measurement indicators can be verified by correlating them to other, independent measures, or the procedures of

obtaining data can be carefully and critically examined. Also, systematic reporting of the measures during an extended period of time will contribute to their reliability.

- How should the information be communicated and displayed, and in what types of documents should the performance data be reported? The data should be presented and communicated clearly and precisely.
- What are the costs and feasibility of obtaining and reporting performance information? Collection of performance measurements can be costly, especially if unsystematic, ad hoc procedures are employed.

The IV&V or Security Assessment Team will implement an array of performance metrics to assess performance and planning processes. Implied within every stage of the planning process is the ability to determine progress made toward established goals or targets. This assessment ability is a monitoring function that simply tracks activities. It may be as simple as a “to do” list or as complicated as a POA&M. Also implied within the planning process is the ability to measure the effectiveness of the actions taken in the conduct of the IV&V or Security Assessment organization’s business. Performance assessment is not merely an end-of-year task, but it is an integral part of the management process itself.

The IV&V or Security Assessment Team will define performance measures based on the project IV&V or Security Assessment Plan and use of the respective IV&V or Security Assessment conduct and reporting standards and procedures. The IV&V or Security Assessment Team will utilize performance measurement metrics that can be verified with “objective evidence,” in addition to customer satisfaction measures. The measurement of IV&V Team or Security Assessment effectiveness will include an evaluation of the timeliness and quality of deliverables, as well as flexibility of the IV&V or Security Assessment Team.

The performance assessment provides the ability to introduce improvements in both process and plan execution by incorporating knowledge gained from the previous planning cycle. It will show what worked as well as what could be improved. The IV&V or Security Assessment Team will aggressively use performance results and information feedback to improve the process and adjust the strategic plan as the program progresses. Performance measures may be reflected in monthly status reports, or in a quarterly technical report. See Sections 5.2.2.4 and 5.2.2.16 for a description of these report formats.

6.2.1 Performance Assessment Areas

IV&V and Security Assessment performance reporting will describe three mandatory assessment areas relating to the IV&V or Security Assessment Team’s performance:

- Technical (quality)
- Schedule (timeliness)
- Business relations (customer evaluation)

Technical and schedule ratings will reflect how well the IV&V or Security Assessment Team complied with the specific contract performance standards. The third assessment area, business relations, recognizes that, when dealing with Federal Student Aid, the IV&V Team may have more than one customer. Accordingly, business relations evaluate the working relationships

between the IV&V or Security Assessment Team and the contract administration team. Some of the other requirements of the contract not directly related to schedule and performance include:

- User satisfaction
- Integration and coordination of all activity needed to execute the contract
- The IV&V or Security Assessment Team's history of professional behavior with all parties

Examples of technical and schedule assessment indicators include the following:

- Effective deliverable status system
- Deliverables on/before due date
- Document reviews performed and completed checklists provided, as applicable

An IV&V or Security Assessment Contractor Evaluation Survey will be submitted periodically by Federal Student Aid and used to assess the IV&V Team's products and processes. The Performance Questionnaire is provided in Appendix H. The IV&V or Security Assessment Contractor may also periodically submit evaluation surveys to the users as a means of assessing the Contractor's effectiveness and getting feedback. The results of this survey will generally be summarized in the form of a memorandum, as described in Section 5.2.2.6. Examples of these survey questions are included in table format in Appendix H and include the following:

Within the scope of the IV&V or Security Assessment involvement:

- Did the IV&V or Security Assessment Team contribute to the reduction of risk? Did they identify risks and formulate and implement risk mitigation plans?
- Did the IV&V or Security Assessment Team identify and apply resources required to meet schedule requirements?
- Did the IV&V or Security Assessment Team assign responsibility for tasks/actions as expected?
- Was the IV&V or Security Assessment Team responsive to ad hoc meetings?
- Was the IV&V or Security Assessment Team flexible and adaptive to schedule changes, etc.?
- Did the IV&V or Security Assessment Team communicate appropriate information to affected program elements in a timely manner?
- Did the IV&V or Security Assessment Team provide best practices or lessons learned?
- Were the IV&V or Security Assessment Team personnel cooperative?
- Were the IV&V or Security Assessment Team's documents free of spelling errors or clerical defects, thorough and complete – was the information accurate?
- Was the interim feedback provided to Federal Student Aid timely and relevant?
- Were reports delivered either on or ahead of schedule – were reports delivered after the scheduled review meeting?

- Was program planning/management adequate – assignment of personnel, recognition of critical problem areas, cooperative and effective working relationships, effective resource use, response to new tasks, and notification of personnel changes?
- Did the IV&V or Security Assessment Team support avoid disruption of internal lifecycle processes and procedures?
- Did the IV&V or Security Assessment Team’s activities avoid delays in established schedules and development planning?
- Did the IV&V or Security Assessment Team personnel interact professionally with Government and contractor personnel?

Depending on the answers to these questions, positive and negative points may be assigned to create a total score for the evaluation.

6.2.2 Performance Assessment Ratings

For technical and schedule ratings, the IV&V or Security Assessment Team will provide information on planned deliverable schedule adherence and quality control of individual deliverables. Objective evidence will include status reports and other work products delivered to Federal Student Aid, as well as the IV&V or Security Assessment Team’s internal configuration control items as described in Sections 5.1.1 and 5.1.2. These include document review schedules and deliverable files.

For the IV&V or Security Assessment Contractor Evaluation Survey, each performance rating area may be assigned one of five ratings: exceptional (1), very good (2), satisfactory (3), marginal (4), or unsatisfactory (5) as listed below. The ratings given by Federal Student Aid (or representatives) should reflect how well the IV&V or Security Assessment Team met the schedule and performance expectations of the contract and the business relationship. A critical aspect of the assessment rating system described below is the second sentence of each rating, which recognizes the IV&V or Security Assessment Team’s resourcefulness in overcoming challenges that arise in the context of contract performance.

Exceptional. Performance exceeds many expectations. The performance of the indicator being assessed was accomplished with no problems, or with a few minor problems for which corrective actions taken by the IV&V or Security Assessment Team were highly effective.

Very Good. Performance exceeds some expectations. The performance of the indicator being assessed was accomplished with some minor problems for which corrective actions taken by the IV&V or Security Assessment Team were effective.

Satisfactory. Performance meets expectations. The performance of the indicator contains some minor problems for which proposed corrective actions taken by the IV&V or Security Assessment Team appear satisfactory, or completed corrective actions were satisfactory.

Marginal. Performance does not meet some expectations. The performance of the indicator being assessed reflects a serious problem for which the IV&V or Security Assessment Team has not yet identified corrective actions. The IV&V or Security

Assessment Team's proposed actions appear only marginally effective or were not fully implemented.

Unsatisfactory. Performance does not meet any expectations and recovery is not likely in a timely or cost effective manner. The performance of the indicator contains serious problem(s) for which the IV&V or Security Assessment Team's corrective actions appear or were ineffective.

6.3 IV&V Metrics

A part of the IV&V performance standards and procedures is to, on a monthly basis, report on IV&V assigned metrics in a clear and concise way that accurately captures the level of effort expended by the IV&V Team members within various assigned Federal Student Aid tasks. This monthly metrics report is intended to present, in clear, plain English, what areas of IV&V work were assessed, and specifically how the metrics are scored. This information will be provided to members of the Federal Student Aid team for further analysis.

IV&V's approach to assigning internal performance metric values is based on the following areas of IV&V work:

- Reviewing of artifacts: documents, code, Web sites, electronic presentations; and recording of actual defects against these artifacts.
- Reviewing of compliance standards: process-oriented (to include security), development contractor's change management process, and configuration management control procedures.

6.3.1 Methodology

The methodology used by IV&V in assessing its own metrics performance is based on the Department of Education's proposed LCM (Lifecycle Management) "framework." Using this agency-defined approach, IV&V traces each of the assigned metrics to the department's lifecycle phases in this model. The LCM is broken down into the stages of:

- (a) Vision
- (b) Definition
- (c) Construction & Validation
- (d) Implementation
- (e) Support and Improvement, and
- (f) Retirement

IV&V recognizes the importance of accurately and realistically using the same evaluation criteria for assessing all IV&V work, thereby ensuring the metrics are consistently comparable across different Federal Student Aid projects. The following are the basic "ground rules" IV&V adheres to in assessing their own performance as to their review and commenting on documents and standards:

- When appropriate, “like” comments will be combined; for example, if a defect occurs in multiple places, this would be combined into one comment with the different references included. (IV&V also makes an effort to avoid counting multiple comments or defects.)
- Only new issues and risks would be included for the month in which they were introduced.

6.3.2 Reporting

The following table (Table 6-1) presents the metric categories, and their associated definitions, used in reporting the IV&V metrics.

NOTE: For consistency, all assigned metric values with a “1” represent a **major** impact or discrepancy, a “2” represents a **moderate** impact or discrepancy, and a “3” represents a **minor** impact or discrepancy.

Table 6- 1, IV&V Metrics Categories

Category	LCM Stage Metric Category Definition
Vision	
V1	Major impact to critical aspects of the defined system vision, requiring immediate resolution to vision products or processes.
V2	Moderate impact to defined system vision, requiring a resolution to vision products or processes by the next scheduled review cycle.
V3	Minor impact to defined system vision, requiring a resolution to vision products or processes by the next scheduled formal review task.
Definition - Requirement	
DR1	Major defect in defined requirements that either fail to meet an organization’s stated critical business needs, or the requirement statement is not constructed to meet industry standards. Both situations require immediate resolution.
DR2	Moderate defect in defined requirements that either fail to meet an organization’s stated business needs, or the requirement statement is not constructed to meet industry standards. Both situations require resolution by the next requirements review session.
DR3	Minor defect in defined requirements that require a resolution before final requirements acceptance.
Definition - Design	
DD1	Major impact to system design, which fails to meet critical aspects of a system requirement, requiring immediate resolution.
DD2	Moderate impact to system design, that either partially fulfills a requirement or fails to address aspects of a system requirement, and requires a resolution by the next scheduled update of the design documentation.
DD3	Minor impact to system design that requires a resolution by next design phase or delivery of final design documentation.
Definition - General	
DG1	Major discrepancies occurring within the Definition phase, not related to either a requirement or design issue, requiring immediate resolution.
DG2	Moderate discrepancies occurring within the Definition phase, not related to either a requirement or design issue, that require a resolution by the next scheduled update task.
DG3	Minor discrepancies occurring within the Definition phase, not related to either a requirement or design issue, which require a resolution by the next design phase of delivery of final requirements / design documentation.

Category	LCM Stage Metric Category Definition
Construction & Validation (Build / Acquisition)	
CVBA1	Major impact to build / acquisition of proposed solution (developed code, acquired COTS), not meeting critical aspects of system requirements or design, requiring immediate resolution.
CVBA2	Moderate impact to build / acquisition of proposed solution (developed code, acquired COTS), not meeting aspects of system requirements or design, and that requires a resolution within the next scheduled task or walkthrough.
CVBA3	Minor impact to build / acquisition of proposed solution (developed code, acquired COTS), that requires a resolution by next major project phase (or delivery of final system solution).
Construction & Validation (Test)	
CVT1	Major discrepancies within proposed system testing solutions that do not meet critical aspects of system requirements, design, or quality standards for respective test artifact, and require immediate resolution.
CVT2	Moderate discrepancies within proposed system-testing solutions that only partially fulfill aspects of system requirements, design, or quality standards for respective test artifact, and that require a resolution by the next scheduled modifications to test products or processes.
CVT3	Minor discrepancies within proposed system testing solutions, which require a resolution by the next major (or final) system modifications to test products or processes.
Construction & Validation (General)	
CVG1	Major discrepancies occurring within the Construction and Validation phase, not related specifically to a system's proposed build and testing solution, and requiring immediate resolution.
CVG2	Moderate discrepancies occurring within the Construction and Validation phase, not related specifically to a system's proposed build and testing solution, which require a resolution by the next scheduled review task.
CVG3	Minor discrepancies occurring within the Construction and Validation phase, not related specifically to a system's proposed build and testing solution, which require a resolution by acceptance of the final system.
Implementation	
I1	Major discrepancies with the planned and actual implementation of the system, not meeting critical aspects of defined implementation processes and products, requiring immediate resolution.
I2	Moderate discrepancies with the planned and actual implementation of the system, not meeting aspects of defined implementation processes and products, that require a resolution within a specific time period (14 days or less) defined by the customer.
I3	Minor discrepancies with the planned and actual implementation of the system, that require a resolution within a specific time period (15 to 45 days) defined by the customer.
Support & Improvement	
S1	Major discrepancies with the planned and actual support of the implemented system, not meeting critical aspects of defined support products and procedures, requiring immediate resolution.
S2	Moderate discrepancies with the planned and actual support of the implemented system, requiring a resolution within a specific time period (30 days or less) defined by the customer.
S3	Minor discrepancies with the planned support of the implemented system, requiring a resolution within a specific time period (31 to 60 days) defined by the customer.

Category	LCM Stage Metric Category Definition
Retirement	
R1	Major discrepancies within the planned and actual retirement of the system, not meeting critical aspects of defined system retirement processes and products, requiring immediate resolution.
R2	Moderate discrepancies within the planned retirement of the system, not meeting aspects of defined system retirement processes and procedures, requiring a resolution within a specific time period (60 days or less) defined by the customer.
R3	Minor discrepancies within the planned retirement of the system, requiring a resolution within a specific time period (61 to 120 days) defined by the customer.

6.3.2.1 IV&V Metrics Report Outline

The following is the outline of IV&V Metrics Report, used in reporting metrics performance on a monthly basis. (The template for this report is included in Appendix E):

Introduction

Methodology - A description of the IV&V methodology used in collecting, assessing, and reporting on QA investigated items and issues.

Summary of IV&V Accomplishments - An overall description of ongoing and planned (new) IV&V activities.

Assessed Deliverables - A listing of those deliverable items that were reviewed, assessed, and commented on by IV&V.

Defect Categories - A table of the metric categories (presented above in the ‘Reporting’ section), and their associated definitions, used for assessing IV&V comments.

Issues and Findings Count - A table of the total counts of the assessed IV&V comments, by their assigned metric categories. An additional breakdown of the counts of the IV&V assessment of comments and issues is also presented, by specific IV&V task area.

6.3.2.2 Metrics Scoring Example

The following is an example of how IV&V “scores” (assigns a metric value to) an IV&V review and comment on a deliverable (in this case, an Intersystem Test Plan):

a) IV&V comment: “Please clarify the phrase ‘Information Development and Dissemination.’ This is something other [test] documentation has not addressed.”

b) Assigned category: Because this deliverable is a test plan, per the agency SDLC, the assigned metric category is the Construction & Validation stage, with the designation of CVT (Construction & Validation – Test)

c) Assigned score: IV&V assesses the severity of this comment as a “2” – Moderate; the assigned metric score is CVT2 (Construction & Validation – Test – Moderate Finding). The IV&V comment is requesting clarification of a phrase, in relation to other delivered test documentation. Though not a major discrepancy, the defect is of a moderate (“2”) severity. Per the CVT2 definition, until this phrase is addressed and fully defined (in

relation to other test documents), the test specification is only “partially” fulfilling “aspects of system requirements, design, or quality standards for respective test artifact, and that require a resolution by the next scheduled modifications to test products or processes.”

6.3.2.3 Enterprise Quality Assurance IV&V Metrics Tracking and Reporting

The Enterprise Quality Assurance Team established these baseline IV&V Metrics in order to measure the effectiveness of IV&V and support process improvement. These metrics are based on IEEE Standard 12207.1-1997, Characteristics of Metrics. Based on this standard the metrics must meet the following requirements:

- Unambiguous: Data is described in terms that only allow a single interpretation.
- Complete: Data includes necessary, relevant requirements with defined units of measure.
- Consistent: There are no conflicts within the data.
- Verifiable: A person or a tool can check the data for accuracy and correctness.
- Traceable: The origin of the data can be determined.
- Presentable: The data can be retrieved and viewed.

The collection of these metrics must have minimal, if any, impact on the business unit development teams. The following metrics are being tracked:

- Customer Satisfaction Survey Results;
- Collection of IV&V contractors’ data in two areas:
 - Count of issues and findings in each lifecycle phase;
 - Count of issues/findings by severity.

The Enterprise QA Team will aggregate and analyze data each month and create a Quarterly Metrics Dashboard report for each IV&V project. An example of this report is included in Appendix I.

Appendix A – Acronyms and Abbreviations

Appendix A: Acronyms and Abbreviations

AC	Access Control (Security Control)
ADA	Americans with Disabilities Act
AT	Awareness and Training (Security Control)
ATO	Authority to Operate
AU	Audit and Accountability (Security Control)
BLSR	Baseline Security Requirements
C&A	Certification & Accreditation
CA	Certification, Accreditation, and Security Assessments (Security Control)
CAN	CVE Candidate
CAP	Corrective Action Plan
CASE	Computer Aided Software Engineering
CBCP	Certified Business Continuity Professional
CCB	Configuration Control Board
CD	Compact Disc
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection Questionnaire
CIPSEA	Confidential Information Protection Security and Efficiency Act of 2002
CIS	Center for Internet Security
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CLIN	Contract Line Item Number
CM	Configuration Management
CM	Configuration Management (Security Control)
CMMI	Capability Maturity Model Integration
CMMI-AM	Capability Maturity Model Integration Acquisition Model
CMP	Configuration Management Plan

CMU	Carnegie Mellon University
COBOL	Common Business-Oriented Language
COCOMO	Constructive Cost Model
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COTS	Commercial Off-The Shelf
CP	Contingency Planning (Security Control)
CR	Change Request
CRG	Certification Review Group
CSAM	Cyber Security Asset Manager
CSCI	Computer Software Configuration Item
CSO	Chief Security Officer
CSQE	Certified Software Quality Engineer
CVBA	Construction & Validation (Build/Acquisition)
CVE	Common Vulnerability Exposure
CVG	Construction & Validation (General)
CVT	Construction & Validation – Test
CY	Current Year
DAA	Designated Approving Authority
DC	District of Columbia
DD	Definition – Design
DG	Definition – General
DR	Definition – Requirement
DRP	Disaster Recovery Plan
DTIC	Defense Technical Information Center
EA	Enterprise Architecture
ED	Department of Education
EDUCATE	Department of Education Federal Student Aid Network
EDSS	Enterprise Development Support Services
EOCM	Enterprise Operational Change Management
ERD	Entity Relationship Diagrams

ESB	Enterprise Service Bus
FDCC	Federal Desktop Core Configuration
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System control Audit Manual
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
FYI	For Your Information
GAO/AIMD	General Accounting Office/Accounting and Information Management Division
GFE	Government Furnished Equipment
GSS	General Support System
HCI	Human Computer Interface
HSPD	Homeland Security Presidential Directive
I	Implementation Metrics
IA	Information Assurance
IA	Identification and Authentication (Security Control)
IAM	Information Security Assessment Methodology
IAM/IEM	Information Security Assessment and Evaluation Methodologies
IAPMP	Information Assurance Program Management Plan
IAS	Institutional Access System
IATO	Interim Authority to Operate
ID	Identification
IEEE	Institute of Electrical & Electronics Engineers
IFAP	Information for Financial Aid Professionals
IG	Inspector General
INFOSEC	Information Security
IP	Internet Protocol
IPR	In Process Review
IR	Incident Response (Security Control)
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization

IT	Information Technology
ITA	Integrated Technical Architecture
IV&V	Independent Verification & Validation
JAD	Joint Application Design
LAN	Local Area Network
LCM	Lifecycle Management Framework
LOA	Letter of Authorization
MA	Major Application
MA	Maintenance (Security Control)
MAJ	Major
MD	Maryland
MIN	Minimum
MOD	Moderate
MOR	Memorandum of Record
MOU	Memorandum of Understanding
MP	Media Protection (Security Control)
N/A	Not Applicable
NE	Northeast
NSA-IAM	National Security Agency INFOSEC Assessment Methodology Certification
NSA-IEM	National Security Agency INFOSEC Evaluation Methodology Certification
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
OOD	Object Oriented Development
OIG	Office of the Inspector General
OM	Office of Management
OMB	Office of Management and Budget
ORR	Operational Readiness Review
OSI	Open Systems Interconnect
OVMS	Operational Vulnerability Management System
P3P	Platform for Privacy References

PE	Physical and Environmental Protection (Security Control)
POA&M	Plan of Actions and Milestones
PBO	Performance Based Organization
PDD	Presidential Decision Directive
PDL	Program Design Language
PDR	Preliminary Design Review
PIP	Performance Improvement Plan
PIR	Post Implementation Review
PL	Public Law
PL	Planning (Security Control)
PM	Project Management
PMI	Project Management Institute
PMP	Project Management Professional
PRR	Production Readiness Review
PS	Personnel Security (Security Control)
PSTN	Public Switched Telephone Network
PUB	Publication
QA	Quality Assurance
R	Retirement Metrics
RA	Risk Assessment (Security Control)
RAD	Rapid Application Development
RAT	Router Audit Tool
RDM	Requirements Database Model
RDM	Requirements Development and Management
RFC	Recommendation for Closure
RIMS	Regulatory Information Management Services
RMA	Reliability, Maintainability, and Availability
RMF	Risk Management Framework
ROE	Rules of Engagement
ROI	Return on Investment
RTM	Requirements Traceability Matrix

RVM	Requirements Verification Matrix
RWL	Risk Watch List
S	Support & Improvement Metrics
SA	System and Services Acquisition (Security Control)
SA	Security Architecture
SAT	Security Assessment Team
SC	System and Communications Protection (Security Control)
SCAP	Security Content Automation Protocol
SDF	Software Development Files
SDLC	Software Development Lifecycle
SDR	System Design Review
SEI	Software Engineering Institute
SI	System and Information Integrity (Security Control)
SLA	Service Level Agreement
SLOC	Source Lines of Code
SNMP	Simple Network Management Protocol
SOO	Statement of Objectives
SOW	Statement of Work
SP	Special Publication
SQL	Standard Query Language
SSID	Service Set Identifier
SSO	System Security Officer
SSP	System Security Plan
ST&E	Security Test & Evaluation
STD	Standard
TIC	Trusted Internet Connections
TRB	Technical Review Board
TRR	Test Readiness Review
U.S.	United States
UCP	Union Center Plaza
V	Vision Metrics

VDC	Virtual Data Center
VDD	Version Description Document
VMS	Virtual Memory System
WAN	Wide Area Network
WBS	Work Breakdown Structure
WEP	Wired Equivalent Privacy
Y/N	Yes/No
YY	Year

Appendix B – Glossary

Appendix B: Glossary

Term	Definition
Acceptable Risk	Acceptable risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Acceptance Test	Formal testing conducted to determine whether or not a system satisfies its user acceptance criteria and to enable the customer to determine whether or not to accept the system.
Accreditation	Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also Authorization to Process, Certification and Designated Approving Authority.
Anomaly	Anything observed in the documentation or operation of software that deviates from expectations based on previously verified products or reference documents. A critical anomaly or defect is one that must be resolved before the verification and validation effort proceeds to the next life cycle phase. Also called an Incident.
Anomaly Report	A report that identifies a program that is not in conformance with design specifications or that is causing mission degradation because of its design. These may be used to document anomalies as well as proposed enhancements. Also called an Incident Report.
Audit	An independent examination of a work product or set of work products to assess compliance with specifications, standards, contractual agreements, or other criteria.
Authorization to Process	Authorization to process occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk associated with it. See also Accreditation, Certification, and Designated Approving Authority.
Availability Protection	Protection of system availability requires backup of system components and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical, time and attendance, financial, procurement, or life-critical applications.
Baseline	A specification or product that has been formally reviewed and

Term	Definition
	agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures.
Build and Test	The software development life cycle phase during which the detailed design is converted into a language that is executable by a computer. This is also called the Implementation Phase.
Capacity Testing	Attempts to simulate expected customer peak load operations in order to ensure that the system performance requirements are met. It does not necessarily exercise all of the functional areas of the system, but selects a subset that is easy to replicate in volume. It will ensure that functions which are expected to use the most system resources are adequately represented.
Capability Maturity Model	Describes the principles and practices underlying software process maturity and is intended to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes.
Certification	Certification is synonymous with the phrase “authorization to process.” Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meet a pre-specified set of security requirements.
Confidentiality Protection	Protection of confidentiality requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.
Configuration Control	An element of configuration management, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.
Configuration Control Board	A group of people responsible for evaluating and approving/disapproving proposed changes to configuration items, and for ensuring implementation of approved changes.
Configuration Item	An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.
Configuration Management	A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance

Term	Definition
	with specified requirements.
Construction and Validation Stage	The objective of the LCM Construction and Validation Stage is to build, test and validate the solution, transform specifications developed in the previous stage into an executable solution and validate solution functionality to ensure it meets or exceeds business and technical expectations.
Critical Defect	An error, omission, or other problem found with the review materials which impacts the ability of the document to achieve the defined scope.
Critical Design Review	A review conducted during the Construction Phase to verify that the detailed design of one or more configuration items satisfies specified requirements; to establish the compatibility among the configuration items and other items of equipment, facilities, software, and personnel; to assess risk areas for each configuration item; and, as applicable, to assess the results of productibility analyses, review preliminary hardware product specifications, evaluate preliminary test planning, and evaluate the adequacy of preliminary operation and support documents. The end result of this review is an approved detailed design of the system.
Defect	A flaw in a system or system component that causes the system or component to fail to perform its required function.
Definition Stage	The Definition Stage is the period of time during which the Business Case Requirements are further defined into business, functional and security requirements that address both the business and technical solution. In addition the project team will develop a high-level functional design and detailed solution design to be used in the Construction and Validation Stage.
Designated Approving Authority (DAA)	The DAA is the senior management official who has the authority to authorize processing (accredit) an automated information system and accept the risk associated with the system.
Detailed Design	The period of time in Construction Phase during which the detailed designs for architecture, software components, interfaces, and data are created, documented, and verified to satisfy requirements.
Deviation	A departure from a specified requirement. A written authorization, granted prior to the manufacture of an item, to depart from a particular performance or design requirement for a specific number of units or a specific period of time.
Entrance/Exit Criteria	Conditions that need to be satisfied for a phase or product to start and to be considered complete, respectively.

Term	Definition
Firewall	A firewall is a system (or network of systems) specially configured to control traffic between two networks. A firewall can range from a packet filter to multiple filters, dedicated proxy servers, logging computers, switches, hubs, routers and dedicated servers.
Functional Configuration Audit	An audit conducted to verify that the development of a configuration item has been completed satisfactorily, that the item has achieved the performance and functional characteristics specified in the functional or allocated configuration identification, and that its operational and support documents are completed and satisfactory.
Gateway	A gateway is a secured computer system that provides access to certain applications. It cleans outgoing traffic, restricts incoming traffic and may also hide the internal configuration from the outside.
General Support System (GSS)	A GSS is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
Implementation Stage	The purpose of the Implementation Stage is to install the new or enhanced solution in the production environment, train users, convert data as needed and transition the solution to end-users. This is the stage where the hardware and/or software product goes into production and, if appropriate, is evaluated at the installation site to ensure that the product performs as required.
Independent Verification and Validation	Verification and validation of a software product by an organization that is both technically and managerially separate from the organization responsible for developing the product.
Individual Accountability	Individual accountability requires individual users to be held responsible for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.
Information Security	Information security is the preservation of confidentiality, integrity, and availability. Each of these attributes is defined as follows: Confidentiality – ensuring that information is accessible only to those authorized to have access Integrity – safeguarding the accuracy and completeness of

Term	Definition
	information and processing methods
	Availability – ensuring that authorized users have access to information and associated assets when required
Integrated Product Team	A multidisciplinary teamwork approach consisting of representatives from all appropriate functional disciplines working together with a team leader to build successful and balanced programs, identify and resolve issues, and make sound and timely decisions.
Integration Test	The period of time in the life cycle during which product components are integrated and the product is evaluated to determine whether target system requirements have been satisfied. The focus of this test is on how multiple components work together and the functions of the system. It will also test the user screens and system interfaces.
Iteration	The process of repeatedly performing a sequence of steps.
Issue	A problem or concern which can't be directly addressed by modifying the review materials. It may affect another unit or group, or other products, and may contain recommendations for future improvements.
Lessons Learned	Summary of the problems encountered during a project, attempted solutions, and the resulting failures and successes. The summary should include the failure or success of the project tools, procedures, and methods.
Life Cycle Model	A framework containing the processes, activities, and tasks involved in the development, operation and support of a system, spanning the life of the system from the definition of its requirements to the termination of its use.
Life Cycle Phase or Stage	Any period of time during software development or operation that may be characterized by a primary type of activity (such as design or testing) that is being conducted. [<i>Note: These stages may overlap one another; for IV&V purposes, no stage is concluded until its development products are fully verified.</i>]
Major Application	A major application is a system that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to

Term	Definition
	support a specific mission-related function.
Metric	A quantitative measure of the degree to which a system, component or process possesses a given attribute.
Minor Defect	An error, omission, or other problem found with the review materials whose impact appears to be minimal.
Modified Waterfall Methodology	<p>There are different versions of this method but they may approach the problem by modifying the traditional "pure" waterfall approach by allowing the steps to overlap, reducing the documentation, and allowing more regression. Some of the more useful versions are:</p> <p>Overlapping Waterfall - steps overlap allowing discovery and insight in later stages; i.e. the requirements analysis may still be occurring partway into the Detailed Design stage. This mirrors many real-life projects.</p> <p>Waterfall with Subprojects - the architecture is broken into logically independent subsystems that can be done separately and integrated together later in the project. This allows each subproject to proceed at its own pace rather than having to wait for all subprojects to have reached the same stage or readiness before proceeding to the next stage.</p> <p>Waterfall with Risk Reduction - a risk reduction spiral (see Spiral Development below) is introduced at the requirements stage and/or the architectural stage.</p>
Module	A program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading. Note: The terms 'module', 'component', and 'unit' are often used interchangeably or defined to be sub-elements of one another in different ways depending on the context.
Networks	Networks include a communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area networks or wide area networks, including public networks such as the Internet.
Operational Controls	Operational controls address security mechanisms that are primarily executed by people (as opposed to systems).
Packet Filter	A packet filter stops or allows packets to flow between two networks according to predefined rules. A simple packet filter is a router. It works on the network layer of the Open Systems Interconnect (OSI) model.
Performance Test	The period of time in the system/software development life cycle during which the response times for the application are validated to be acceptable. The tests ensure that the systems environment will support production volumes, both batch and

Term	Definition
	on-line.
Physical Configuration Audit	An audit conducted to verify that a configuration item, as-built, conforms to the technical documentation that defines it.
Post Implementation Review	A milestone review to evaluate the project outcome to verify whether the project achieved the desired results and met predicted strategic outcome measures within the planned cost and schedule.
Preliminary Design Review	A review conducted during the Definition Phase to evaluate the progress, technical adequacy, and risk resolution of the selected top level design approach for one or more configuration items; to determine each design's compatibility with the requirements for the configuration item; to evaluate the degree of definition and assess the technical risk associated with the selected manufacturing methods and processes; to establish the existence and compatibility of the physical and functional interfaces among the configuration items and other items of equipment, facilities, software and personnel; and, as applicable, to evaluate the preliminary operational and support documents.
Prototyping Methodology	The system concept is developed as the development team moves through the project by developing and demonstrating part of the system, usually the most visible part, to the customer. Modifications may be made and the next part is then developed based on feedback from the customer. At some point, agreement is reached between the customer and the developer that the prototype is satisfactory and outstanding work is finished and the system delivered.
Preliminary System Design	The portion of the Definition Phase during which the top level designs for architecture, software components, interfaces, and data are created, documented, and verified to satisfy requirements.
Production Readiness Review	A review conducted to review feedback from customer sponsors and to review system performance compared to anticipated value and success measures. The review assesses the readiness of technology infrastructure, as well as the readiness of affected organizations.
Proxy	A proxy is a program which allows/disallows access to a particular application between networks. It works on the Application layer of the OSI model.
Rapid Application Development Methodology	Rapid Application Development Methodology is a term often used without being clearly defined. It may mean rapid prototyping to one user, the use of CASE tools and tight deadlines to another or a headline article in a trade journal to a

Term	Definition
	third. As a useful term in a strategic sense, the best usable definition is that RAD means a project that requires an accelerated development environment compared to more traditional project modes and timelines. It requires more careful management and better understanding of the risks involved. Using this definition frees RAD of association with any one set of tools and focuses on the relationship between software development methods within specific environments especially in relation to time constraints.
Regression Testing	The rerunning of test suites that a program has previously executed correctly in order to detect errors created during unrelated software correction or modification activities.
Retirement Stage	The purpose of the Retirement Stage is to execute the systematic termination of the system and preserve vital information for future access and or reactivation.
Risk	Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.
Risk Assessment	Risk assessment is the structured analysis of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.
Risk Management	An approach to problem analysis which weighs risk in a situation by using risk probabilities to find a more accurate understanding of the risks involved. Risk management includes risk identification, analysis, prioritization, and control.
Rules of Behavior	These are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability.
Sensitive Information	Sensitive information refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

Term	Definition
Sensitivity	Sensitivity in an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability. This level is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.
Software Development	A set of activities that results in software products. Software development may include new development, modification, reuse, reengineering maintenance, or any other activities that result in software products
Software Development Folder	A repository for material pertinent to the development of a particular body of software. Contents typically include (either directly or by reference) considerations, rationale, and constraints related to requirements analysis, design, and implementation; developer-internal test information; and schedule and status information. The contents are usually stored on EDUCATE or within a development tools such as the Rational Suite.
Software Life Cycle	Period of time from software product conception to when the software is no longer available for use. The software life cycle typically includes a concept design phase, system requirements analysis phase, preliminary and detailed design phases, build and test phase, integration and acceptance test phases, and a system deployment phase.
Software Process Assessment	Appraisal to determine the state of an organization's current software development process, to determine the high-priority software process-related issues facing an organization, and to obtain the organizational support for software process improvement.
Spiral Development Methodology	This is a risk-oriented method that breaks a project into smaller "mini-projects". Each mini-project focuses on one or more identified major risks in a series of iterations until all risks have all been addressed. Once all the risks have been addressed, the spiral model terminates the same way the waterfall model does.
Staged Delivery Development Methodology	This bears some similarities to both Prototyping and Waterfall with Subprojects in that software is demonstrated and delivered to the customer in successive stages. The steps up to and through architectural design are the same as the Traditional Waterfall and the following build and deliver steps are done for each of the separate stages. It differs from Prototyping in that the scope is established at the beginning of the project and the software is delivered in stages rather than in

Term	Definition
	one package at the end as is done with the waterfall method. It differs from Waterfall with Subprojects in that the stages are delivered independently rather than integrated towards the end of the project.
Standards	Guidelines employed and enforced to prescribe a disciplined, uniform approach to software development and its associated products.
Support and Improvement Stage	The System Support and Improvement Stage is the period of time during which Federal Student Aid system upgrade or iteration is evaluated from an operational and maintainability standpoint.
System	System is a generic term used for brevity to mean either a major application or a general support system.
System Operational Status	System operational status is either: (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.
System Requirements Review	A review conducted to evaluate the completeness and adequacy of the requirements defined for a system; to evaluate the system engineering process that produced those requirements; to assess the results of system engineering studies; and to evaluate system engineering plans.
System Test	The System Test is the period of time in the life cycle during which the product is evaluated to determine whether functional and performance requirements have been satisfied.
System Trouble Report	A report that identifies a program that is not in conformance with design specifications or that is causing mission degradation because of its design. These may be used to document anomalies as well as proposed enhancements. Also called an Incident Report.
Target System	The target system is the subject of the security assessment.
Technical Controls	Technical controls consist of hardware and software controls used to provide automated protection to the system or applications.
Test Readiness Review	A milestone review to determine that the software test procedures for each configuration item are complete and to ensure that the software developer is prepared for software performance testing. Entry criteria are reviewed and verified to be complete. Examples include Integration Test Readiness Review, Acceptance Test Readiness Review, and Production Test Readiness Review.

Term	Definition
Threat	Threat is an activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.
Traceability	Degree to which a relationship can be established between two or more products of the development process, especially products having a predecessor, successor, or master-subordinate relationship to one another (e.g., the degree to which the requirements and design of a given software component match).
Unit	The lowest element of a software hierarchy that contains one or more of the following characteristics: (1) a unit comprising one or more logical functional entities, (2) an element specified in the design of a computer software component that is separately testable, (3) the lowest level to which software requirements can be traced, and (4) the design and coding of any unit can be accomplished by a single individual within the assigned schedule.
Unit Test	The process of ensuring that the unit executes as intended. This usually involves testing all statements and branch possibilities.
Validation	Determination of the correctness of the final program or software produced from a development project with respect to the user's needs and requirements. Validation answers the question, "Am I building the right product?"
Verification	The process of determining whether the products of a given phase of the software development cycle fulfill the requirements established during the previous phase. Verification answers the question, "Am I building the product right?"
Vision Stage	The Vision Stage is the initial system lifecycle stage during which project scope, high-level requirements and user needs are documented and evaluated.
Vulnerability	Vulnerability is a flaw or weakness that may allow harm to occur to an automated information system or activity.
Walkthrough	An informal review conducted to assess the development approach, the product and engineering practices applied, the completeness and correctness of capabilities and features, and the rules of construction for the target system products. Examples of specific types of walkthroughs include requirements walkthroughs, design walkthroughs, and source code walkthroughs.

Term

Waterfall Development
Methodology

Definition

In this model, the oldest and still one of most commonly used, the project proceeds through a series of separate sequential steps starting with the concept and ending with implementation. There is usually a review at the end of each step to determine if it is acceptable to proceed to the next step. If it is found that the project is not ready to proceed, the project is held in the current step until it is ready. In the pure form of this methodology, the different steps do not overlap.

Appendix C - IV&V Checklists

Appendix C: IV&V Checklists

Standard checklists are fundamental tools maintained by the IV&V Team for use during evaluations. They may be used as is, or tailored as necessary.

Checklist Name	Checklist Description
Document Review Checklist	This checklist is used as a generic checklist for documentation reviews and should be tailored to match the type of document under review. It is an aid to determining the overall quality of a document as to readability, utility, correctness, and completeness.
Requirements Review Checklist	This checklist is used to determine whether a given concept, set of requirements, design, test, etc., demonstrates that a CSCI or system satisfies its specified acceptance requirements.
Preliminary Design Checklist	This checklist is used to aid in assessing the top-level design as well as the allocation of requirements to software components, and to determine whether the Preliminary Design Review resolved open issues concerning the handling of high-level design requirements.
Detailed Design Checklist	This checklist is used to aid in determining if all the software requirements have been translated into a viable software design, and whether the Critical Design Review resolved open issues concerning the handling of critical requirements
Process Review Configuration Management Checklist	This is a sample process review checklist with an emphasis on Configuration Management practices. This checklist is used to determine whether Configuration Management Procedures document and implement plans for: performing configuration control; providing access to documentation and code under configuration control; and controlling the preparation and dissemination of changes to master copies of software and documentation so they reflect only approved changes.
Code Review Checklist	This checklist suggests evaluation criteria used to determine whether the software design has been correctly implemented in code that adheres to programming standards and conventions.
Unit Testing Review Checklist	This checklist is used to determine whether: adequate test procedures to test each Computer Software Unit were developed and documented; each unit was coded and tested ensuring that the algorithm(s) and logic employed are correct and satisfy the specified requirements; all necessary revisions to the design documentation and code were made; all necessary retesting was performed; and test results were recorded.
Software Development Files Review Checklist (Department of Education Federal Student Aid Network)	This checklist is used to determine whether Software Development Files contain material pertinent to the development or support of the software including: requirements, design considerations, constraints, documentation, program design language and source code, test data; status information; and test requirements, cases, procedures, and their results.

Checklist Name	Checklist Description
Test Readiness Review Checklist	This checklist is for evaluating the Test Readiness Review to ensure that adequate preparations were taken for the performance of System Integration Test, and System Acceptance Testing.
Section 508 Review Checklist	This checklist is for performing a Section 508 assessment. It is included here to provide guidance to the IV&V Team as to the Section 508 requirements.

Document Review Checklist

The purpose of document reviews is to verify that the technical documents and plans are consistent with project plans, requirements and guidelines established by Federal Student Aid. This checklist must be tailored for each document, but sample product assessment guidelines are provided.

Document Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
1	Is the document written to the appropriate level of detail?		
2	Is the document consistent with other predecessor documents?		
3	Is the material within this document feasible as stated?		
4	Are all required paragraphs included in the document? (Is the document compliant with data item description or standard)? Add tailoring here to meet standard.		
5	Are all sections in the proper order?		
6	Does each section in the proper order?		
7	Is the document in compliance with required statement of work? Contract Data Requirements List? Contract?		
8	Are all statements compatible and consistent?		
9	Is the level of detail and presentation style consistent throughout the document?		
10	Are all terms, acronyms and abbreviations defined?		
11	Is the overall approach sound?		
12	Is the document well researched and based on proven prototypes?		

Requirements Review Checklist

The purpose of this checklist is to provide guidance for verifying the quality of the system requirements against consistent criteria.

Requirements Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Requirements	
1	Completeness: All requirements have been allocated.		
2	Correctness: Each stated requirement represents something required by the system.		
3	Consistency: Each requirement is internally/externally consistent with other requirements.		
4	Traceability: The origin of the stated requirement is clear.		
5	Testability:		
	a. An objective and feasible test can be designed to determine whether the requirement has been met.		
	b. Requirements are specified in quantitative terms that are measurable.		
	c. The requirement is annotated with an associated qualification method.		
6	Understandability: Terminology is understandable and consistent. Notations are accurate.		
7	Nonambiguous:		
	a. The stated requirement has only one interpretation.		

Requirements Review Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Criterion	(Y/N) Record References to Non-Compliant Requirements	
	b. The use of vague qualifiers is avoided (e.g., "...to the extent practical...", "A minimum of...").		
	c. The requirement has a unique identifier.		
	d. Proper requirements language is used (i.e., "shall").		
8	All relevant equipment is identified and described (e.g., processors, memory, interface hardware, and peripherals).		
9	The software role in the system is explained. Major software functions are described in relation to system operation.		
10	The hierarchy of functions (or the organization of objects) is supported by enough data to demonstrate traceability of inputs and outputs.		
11	The document structure is consistent with the hierarchy of functions (or partitioning of objects).		
12	The data flow is consistent with inputs and outputs. Sources and destinations for all data are identified.		
13	Each identifiable requirement defines a testable function (e.g., makes a decision, controls a subordinate function, or moves or computes data).		
14	Requirements specify behavior under normal and abnormal conditions.		
15	Sequences are clearly defined.		

Requirements Review Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Criterion	(Y/N) Record References to Non-Compliant Requirements	
16	Accuracy/precision is stated where necessary.		
17	There are no unwarranted design constraints.		
18	Performance characteristics are reasonable.		
19	Resources are budgeted realistically (e.g., memory, throughput, response times, and data storage).		
20	The scope of the requirements is consistent with software estimates, schedules, and support plans.		

Preliminary Design Checklist

The purpose of design reviews is to determine whether all software requirements have been translated into a viable software design. Generally, software projects have two design phases: top-level and detailed design. The following checklist applies to the high level design.

Preliminary Design Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
1	The functional [or object] partition is consistent with the Software Requirements and Interface Requirements.		
2	Security, Reliability, Maintainability, Availability issues have been addressed.		
3	Each function has a single well defined purpose.		
4	Software Requirements Specification and Interface Requirements Specification allocated to code.		
5	The Requirements Allocation Matrix has been updated to reflect allocation of requirements to source code including commercial off-the shelf, if applicable.		
6	All inputs, outputs, functional control and sequencing should be defined.		
7	Internal interfaces and external interfaces are defined.		
8	Commercial off-the-shelf applications and interfaces are defined.		
9	Human factors have been addressed where relevant.		
10	Contractor configuration management procedures and controls are in place.		

Detailed Design Checklist

The purpose of detailed design reviews is to determine whether all software requirements have been translated into a viable software design. Generally, software projects have two design phases: top-level and detailed design. The following checklist applies to the detailed design.

Detailed Design Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
1	Each module has a single, clearly stated function.		
2	Units are named according to applicable conventions.		
3	There is a software requirement from which the need for this function arose.		
4	There is no superfluous processing.		
5	No necessary processing is missing.		
6	There are no other types of identifiable errors in logic.		
7	There are no possible error conditions that were not provided for.		
8	Unit interfaces are consistent and well defined.		
9	Software requirements can be traced to code.		

Process Review (Configuration Management) Procedures Checklist

The purpose of a process review is to ascertain, based on objective evidence, that approved plans and procedures have been implemented and are being followed.

Process Review (Configuration Management) Procedures Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
1	There are documented processes in use that provide timely, comprehensive, and accurate processing, reporting, and recording of approved changes to controlled components.		
2	There are documented processes that provide comprehensive implementation of approved changes and dissemination of corrected documentation and software changes.		
3	There are documented processes in use that provide accurate reporting and recording for the status of all proposed changes and change resolution.		
4	There are documented processes in use that provide verification and implementation of identification, change control, and status accounting of descriptive documentation and software materials.		
5	There is an internal baseline for documentation. (In the "Notes" section, record contract items (e.g., contract data requirements lists which have been placed under internal control. Note any items which should be under control, but are not, as of the review date.)		
6	There are documented processes in use which govern the identification (titling, labeling, numbering, and cataloging) of all software documentation and software materials:		

Process Review (Configuration Management) Procedures Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
	a. Identification denotes the component to which it applies.		
	b. The purpose is described.		
	c. The applicable baseline is defined.		
	d. The serial, edition, and change status is identified.		
	e. The compilation date for each deliverable software component is identified.		
	f. There is visual and machine readable identification for all delivered software media that permits direct correlation with delivered documentation.		
7	There are documented processes in use that govern internal control of all documents and software materials in the development support library.		
8	There are documented processes in effect that require bringing each component of the software under configuration control.		
9	There is a documented process that governs the establishment of the Configuration Control Board.		
10	The Configuration Control Board operates, with the proper membership, as described in the documented process.		
11	There are verifiable records indicating that all required Configuration Control Board members were in attendance at meetings.		
12	There are documented processes		

Process Review (Configuration Management) Procedures Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
	that define the methods and format for submission of problem reports for problems detected in activities and products.		
13	There are documented processes in use that define the methods for processing problem reports for software and documentation which has been placed under configuration control.		
14	There are documented processes in use that control the preparation and dissemination of changes to documentation to reflect approved and implemented changes.		
15	There are documented processes in use that require the generation of a problem report when changes are made to software and baselined documentation.		

Code Review Checklist

The purpose of a code review is to determine whether the software design has been correctly implemented in code that adheres to the programming standards and conventions. The following checklist suggests evaluation criteria and questions to consider when reviewing the code.

Code Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
1	Does the module (unit) have a single, clearly stated function?		
2	From which software requirement(s) did the need for this function arise?		
3	Does the documentation adequately describe the processing, data, and interfaces of this function?		
4	Is the developer name, date of development and description of module function or code change included in the comments? Are comments adequate and accurate in describing the processing? Do comments concentrate on what is being done as opposed to how it is being done?		
5	Are there control flow errors?		
6	Is there superfluous or dead code?		
7	Is there missing code?		
8	Are there other types of errors in the logic?		
9	Are there possible error conditions that are not trapped?		
10	Are statements "commented out?"		
11	Does the code conform to Federal Student Aid Programming Standards and Conventions (if applicable)? Does the code adhere to the C or applicable coding standards?		

Code Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
12	Has the code under review been checked into the Federal Student Aid Configuration Management code management tool?		
13	Has the Unit Test Plan for the code under review been completed?		
14	Does the module achieve its goals as stated in the design documentation?		
15	Does the module generally follow the program design language in the design documentation?		
16	Are there obvious style problems that affect readability or maintainability?		
17	Is the file too long (>500 lines) or contain too many functions?		
18	Is there duplicate or similar code that could be combined into a general-purpose function?		
19	Are there obvious code inefficiencies (opening and closing a file multiple times)?		
20	Are there better ways to accomplish the same results provided by the code?		
21	Does the function return correct information to the caller in all cases?		
22	Error cases not handled correctly (including caller program ignoring error status returned by called function)?		
23	Do error messages provide enough information for an operator to understand the problem being reported?		
24	Has a code review results file been created and checked into code		

Code Review Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
	control tool?		
25	Has the Development Lead or his/her designee followed up to ensure that any discovered defects are addressed prior to the completion of testing?		

Unit Testing Review Checklist

The purpose of this checklist is to provide guidance for assessing the quality of unit testing.

Unit Testing Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
Unit Test Plan Review			
1	Is the purpose/objective of the test stated and it is applicable to the unit in question?		
2	Is the requirement reference traceable to the unit?		
3	Is the data recording and analysis method defined?		
4	Are all required software items and tools identified and available?		
5	Is the version of each software item and tool identified?		
6	Is regression analysis defined in case of errors and code update?		
7	Were any tools employed (test path coverage)?		
8	Is the test plan consistent with the prescribed process defined by the development team?		
9	Was the test plan subjected to a peer review?		
10	Will the test be executed by someone besides the author?		
11	Will the test be executed by someone besides the author?		
Unit Test Results Review			
12	Was the test plan approved prior to the start of testing?		
13	Are test results retained in the application folder?		
14	Is there a test report for this unit?		
15	Were the required higher level		

Unit Testing Review Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
	units available?		
16	Were the results reviewed by an independent evaluator?		
17	Is there evidence of source code review prior to the start of testing?		

Software Development Files Review Checklist

The purpose of a software development folder is to track development information for the effort for development, maintenance and training purposes.

Document Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
1	The Software Development File procedures are documented in the Software Development Plan or available on the Department of Education Federal Student Aid Network.		
2	Each software development file contains a cover page describing the description and content of file.		
3	There is a standard format consistent between the folders and the module names and identifiers are correct. Code follows Federal Student Aid coding standards: (e.g. no extensible markup language.)		
4	The software development file contains the following sample Concept Design Phase information as appropriate including: general concept data, results of Concept Design Review, action items and concept documentation in one generic folder.		
5	The software development file contains the following sample System Requirements Analysis phase data including the requirements database or links, System Requirements Review actions and notes and requirements documentation.		
6	The software development file contains the following sample preliminary and detailed design information as appropriate including: Hierarchy Diagrams, functional flow diagrams, program design language, Specifications,		

Document Review Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
	preliminary design review and critical design review data, object oriented diagrams, requirements allocations, Human Computer Interface data, event trace data, design notes action items, and unit test plans.		
7	The software development file contains the following Build and Test information as appropriate including: source code, unit test procedures and results, build test procedures, requirements trace data, and defect tracking.		
8	The software development file contains the following Integration and Acceptance Test information including updated source code, test procedures, requirement allocations, defects, updated design information, test readiness review notes, test results, and regression test procedures and results and deployment data including production readiness review action items if applicable.		

Test Readiness Review Checklist

The purpose of a Test Readiness Review is to assess readiness to proceed to the Integration or Acceptance Test. This checklist provides guidance for assessing these reviews. The standard for Test Readiness Reviews are included in the Enterprise Testing Standards Handbook.

Test Readiness Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
1	Software Test Plan Submitted and approved.		
2	System Integration or Acceptance Test Plans submitted and approved.		
3	Configuration of System under test documented.		
4	Draft Version Description Document submitted three working days before Test Readiness Review.		
5	Requirements/Test Case Traceability completed.		
6	Developmental Software under Configuration Management Control.		
7	Hardware/System Software under Configuration Management Control.		
8	Commercial Off-The Shelf Software under Configuration Management Control.		
9	Test Procedures and Test Data under Configuration Management Control.		
10	All applicable deviations/waivers submitted and approved.		
11	Test Environment established.		
12	Test specific software developed.		
13	Test Dry Runs completed and results submitted. Results included the number of dry run		

Test Readiness Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Criterion	(Y/N) Record References to Non-Compliant Items	
	requirements passed, failed, and not tested.		
14	Test Schedule prepared.		
15	Prior milestones completed (e.g., critical design review) in that all of its exit criteria is satisfied and all Action Items responded to.		
16	Security requirements satisfied.		
17	Entrance Criteria for the Integration/Acceptance/Alpha/Beta Testing established.		
18	Exit Criteria for the Integration/Acceptance/Alpha/Beta Testing established.		

Section 508 Review Checklist

The purpose of the 508 checklist is to provide guidance for the IV&V analyst to ensure that the Federal Student Aid product under review meets the requirements of Section 508 of the Rehabilitation Act.

Section 508 Review Checklist			
IV&V Engineer:			Date:
Project:			Phase:
Item #	Assessment Requirement For Web-Based Application	(Y/N) Comments	
1	Have web accessibility guidelines been established?		
2	If web accessibility guidelines have not been established, is there a timetable for doing so?		
3	Are there procedures in place to ensure that maintenance of the web site and its contents follows the established accessibility guidelines?		
4	If not, is there a timetable for establishing these procedures?		
5	Is clear and detailed information provided on the component-level pages or on the agency wide home page for improving the accessibility of the web site for persons with disabilities?		
6	If not, is there a timetable for providing this?		
7	Is there an e-mail address allowing people with disabilities to inform the agency of accessibility problems and is this address advertised?		
8	If not, is there a timetable for providing this?		
9	Are meaningful text equivalents provided for all non-text elements such as images, multimedia objects, Java applets etc. to allow translation by assistive technologies?		
10	If multimedia is used, is text captioning provided for all audible output?		
11	If multimedia is used, is audible output provided for all important visual information?		
12	If multimedia is used, are audio output and text captions synchronized with their associated dynamic content?		
	Is the page capable of being understood and navigated if users cannot identify specific colors or differentiate between colors?		
	Is the page viewable without style sheets or with the style sheets turned off or not supported by the browser?		
	If style sheets are used, is the page designed so it does not interfere with style sheets set by the individual's browser?		

Section 508 Review Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Assessment Requirement For Web-Based Application	(Y/N) Comments	
	If the page includes server-side image maps, are duplicate text links provided for all links within the server-side image maps?		
	If the page includes server-side image maps, has a timetable been established to replace the server-side image maps with client-side image maps except where regions cannot be defined with an available geometric shape?		
	If the page includes client-side image maps, does each map region have a text equivalent?		
	If the page contains data in tables and if any table has two or more rows (including header or data cells), does each cell provide identification of row and column headers?		
	Are “id” and “header” attributes used to identify table rows and headers within each cell? Newer screen readers can make use of these attributes.		
	Are tables used for formatting text? Note: <i>Section 508 does not prohibit this practice, but discourages it where developers want to make their sites completely accessible.</i>		
	If tables are used for formatting text, are methods used to minimize their effect on accessibility?		
	Are tables created with the use of the <PRE> tag? Note: <i>Section 508 does not prohibit this practice, but discourages it.</i>		
	If frames are used, is there meaningful text describing each frame?		
	Does the page include content that may cause screen to flicker with a frequency between 2mhz and 55mhz?		
	When scripting languages are used and the scripts affect content displayed to the user, is a text equivalent that is accessible to a screen reader provided for the user by the page or the script?		
	If the page uses applets, is the same information and functionality provided in an accessible format?		
	If the page uses other programmatic objects, such as Flash, Shockwave, etc, or otherwise requires the use of plug-ins or programmatic support for the browser, does the page include a link to the plug-in or programmatic item required for accessing the content of the page and is that plug-in or programmatic item itself accessible to people with disabilities?		

Section 508 Review Checklist			
IV&V Engineer:		Date:	
Project:		Phase:	
Item #	Assessment Requirement For Web-Based Application	(Y/N) Comments	
	If the page includes links to Adobe Acrobat files (extension .pdf), were those files created in a way that is likely to maximize their usability for people with disabilities? i.e. the files were created by “printing to .pdf” or scanned into .pdf and run through an optical character reader process and checked for accuracy?		
	If the page contains one or more electronic forms designed for online completion, does each form permit users of assistive technology to access the information, field elements, and functionality required for completion and submission of the form including all directions and cues?		
	If the page contains one or more forms designed to be completed online but that is inaccessible to people with disabilities in some respect, does the page include an accessible form or a link to an alternate accessible form?		
	If the page includes navigational links to other web pages within the same website, is there a link allowing users of screen readers to skip over those links?		
	If the page requires users to respond within a fixed amount of time before the user is “timed out”, is there a signal provided to alert the user that a time out is going to occur and is the user given sufficient time to request more time?		
	If the page being reviewed contains barriers to access for people with disabilities, is there an alternative text-only page that contains the same information and is updated as often as the reviewed page?		
	Has the page been tested by users with disabilities using assistive technology (e.g. screen reader, Lynx browser, IBM Home Page Reader)?		
	If not, is there a timetable for establishing these procedures?		

Appendix D - Risk Management Process

Appendix D: Risk Management Process

ESTABLISH AND MAINTAIN A FORMAL FEDERAL STUDENT AID IV&V PROJECT RISK MANAGEMENT PROCESS

EXECUTIVE SUMMARY

The benefit of formalizing the Federal Student Aid project risk management process will be:

- Identify issues that are actually project risks
- Keep all identified risks easily visible at all times rather than just those risks that are high profile at any one time.
- Encourage the creation of strategies to keep risks from turning into problems
- Track the risks to determine if the risk exposure changes with time
- Track the risks to ensure they are addressed
- Provide a framework for future improvement

The project risk management process described here is not a complete risk management process, but is a simplified version modified for Federal Student Aid. Like all risk management processes, it is a means of codifying behavior usually being done on an ad-hoc basis. As such, it will remain high-level and will be effective insofar as the project personnel assist in identifying project risks and, in particular, help identify strategies to deal with the risks. IV&V proposes to identify these risks as they surface during reviews, status meetings, conversations, etc. In many cases, these are risks already identified by the development team as issues. Once risks are identified, they are assigned a rating based on probability of occurrence, severity of effect, and risk exposure. Strategies to deal with the risk will be formulated where possible and the risk watch list presented to the development team for suggestions and modifications, thereby reducing the effort required of them. The risks will then be tracked through the project until addressed. IV&V will suggest mitigating strategies if none are identified by the project personnel.

RISK MANAGEMENT BACKGROUND

Risk management is a technique that may be applied to many aspects of an information system. In the context of this document, it is a project management tool used to codify good management techniques meant to identify and control the risks inherent in any software development process.

Most software projects use risk management informally and this is usually referred to as “crisis management”. In crisis management, the mechanism for tracking and dealing with risks is ad-hoc and prone to error. Risks get attention when they become problems. It is only recently that risk management techniques have evolved and been elevated to the status of a formal process. In the past, for instance, lifecycle methodologies often assumed that requirements can always be thoroughly determined or that users will fully participate or that project estimates can be accurately determined ahead of time. If these are not true, the textbook approach will often say that the project will not go forward until the developers have received “sign-off.” This often becomes a method of avoiding liability rather than a management tool. Most developers,

however, know that projects do go forward under these circumstances and the risks attendant to them are handled individually and on an ad-hoc basis.

A common risk factor in software development is project estimates based on worst-case or best-case scenarios rather than realistic estimates by knowledgeable individuals. Another common risk is incomplete and/or changing user requirements. One expert's estimate of risk in the area of management information systems (Caper Jones) gives the following figures which, will probably be recognized by most of those involved in software projects:

Risk Factor	Percent of Projects At Risk
Creeping user requirements	80%
Excessive schedule pressure	65%
Low Quality	60%
Cost Overruns	55%
Inadequate configuration control	50%

Risk management is a process for identifying and prioritizing these potential problems, addressing them, and determining means of dealing with them. Done properly, risks are identified before they become problems in a continuous process that monitors the project and identifies risks as they occur. In reality, the QA process itself is a form of risk identification. As software development periods are increasingly collapsed, systems become more complex, and requirements are more difficult to firmly identify early in the lifecycle, risk management assumes greater importance. The methodology known as Spiral Development, for instance, is predicated on constant risk management.

Identifying and dealing with risk is a strategy for reducing project uncertainty. Establishing risk management as a formal on-going process allows attention to be focused on the areas of greatest risk and allows plans to be formulated ahead of time to deal with these risks. It cannot, of course, eliminate risk. If a risk is not identified, for instance, a mitigation strategy cannot be formulated, but if a number of risks have been identified, tracked and dealt with, there will be more resources available to address unidentified risks if they do occur. Making project risk management a continuous process allows risks to be addressed and avoided and allows new risks to be identified and added to the watch list.

In addition to providing a day-to-day project management tool for Federal Student Aid managers, this will lay the groundwork for a full-scale Federal Student Aid project risk management process in the future.

ESTABLISHING THE FEDERAL STUDENT AID PROJECT RISK MANAGEMENT PROCESS

- Identify risks using a structure such as SEI's Taxonomy-Based Risk Identification. In the case of Federal Student Aid, risks will often be identified through reviews, status meetings, and meetings with project personnel.

- Analyze risks, quantifying where possible:
 - The probability of a risk occurring
 - The impact of the risk to the project
 - Cost
 - Performance
 - Schedule
 - Support
 - The overall risk to the project using an Impact/Probability Matrix
- Plan for selected risks
 - Importance of risk
 - Information necessary to track the status of the risk
 - Assign responsibility for Risk Management activity
 - Identify resources necessary to perform Risk Management
 - Define approach for mitigating risk
- Track risks to determine if the risk exposure for a given risk changes with time
- Use mitigation to manage risk

CONSTRAINTS

The open involvement of the project's managers and project personnel in identifying risks during interviews and reviewing the attached Risk Watch List is critical to the success of the process. This entails an investment in resources and cultural and organizational change over time. In the case of Federal Student Aid, it is unrealistic to attempt a complete project risk management process at this point given the ongoing development and the development environment. It is possible, however, to implement the appropriate techniques to identify significant risks, provide a tracking mechanism, and establish a process for identifying proactive strategies.

ATTACHMENT A – RISK WATCH LIST

The Risk Watch List is the tool used for tracking project risks. It contains the identified risk stated in Risk Condition/Consequence format. That is, the risk is stated followed by the consequence to the project if the risk becomes a problem. In addition, there are columns for the estimated probability (“P”) of the risk becoming a problem, the estimated impact (“I”) on the project if the risk becomes a problem, and the Risk Exposure to the project, which is a product of the Probability and the Impact and is determined by the Probability Matrix in Attachment B.

The Risk Watch List provides a tracking mechanism by identifying events (“First Indicator”) that indicate a risk is becoming a problem, the approach determined to mitigate or control the problem, and the date the mitigation approach was identified. This column can also be used to provide status updates.

[Application/Project] IV&V Risk Watch List Open Risks (MM-DD-YY) [Contractor Name].									
ID #	Date	Risk	P	I	Risk Exposure	First Indicator	IV&V Risk Mitigation Approach	Status	Condition
[#]	[mm/dd/yy]	[Provide detailed verbiage to identify risk].	[#]	[#]	[High, medium, low]	[Provide reason that risk was brought to light]	[mm-dd-yy] [Provide description of mitigation approach].	[Open, Closed]	<div style="background-color: red; color: black; padding: 2px; text-align: center;">Red [equals High]</div> <div style="background-color: yellow; color: black; padding: 2px; text-align: center;">Yellow [equals medium/low]</div> <div style="background-color: green; color: black; padding: 2px; text-align: center;">Green [equals closed]</div>

P = Probability of risk becoming a problem
 1- Improbable
 2 – Probable
 3 - Very likely

I = Impact if risk becomes a problem
 1 – Negligible
 2 - Marginal
 3 - Critical
 4 - Catastrophic

* Risk Exposure (determined by exposure matrix comparing Probability and Impact)
 1, 2- Low
 3, 4- Medium
 5, 6- High

ATTACHMENT B – PROBABILITY MATRIX

The risk exposure for any given risk is determined by using the estimated probability of the risk and the estimated impact of the risk to derive a weighted exposure from the matrix. This provides a risk exposure factor based on both probability and impact.

RISK EXPOSURE (PROBABILITY) MATRIX				
		Probability 		
		3- Very Likely	2 - Probable	1- Improbable
Impact 				
	4 - Catastrophic	6 High	5 High	4 Medium
	3 - Critical	5 High	4 Medium	3 Medium
	2 - Marginal	4 Medium	3 Medium	2 Low
	1 - Negligible	3 Medium	2 Low	1 Low

Appendix E - IV&V Reporting Templates

Appendix E: IV&V Reporting Templates

The following templates are provided for use in IV&V task reporting:

Template Name	Template Description
Document Review Schedule	Used to schedule the internal walkthrough.
Document Tracking System Template	Used to track the documents reviewed and their status during the walkthrough.
Walkthrough Meeting Notice	Used to notify the participants that a walkthrough is being held.
Walkthrough Log	Used to record the details of the walkthrough and obtain the next consecutive walkthrough number.
Defect/Issue List	Used to describe the resolution of each defect/issue.
Walkthrough Disposition	Used to document the disposition of the defects/issues.
IV&V Plan	Used to provide a summary of the IV&V Plan.
Review Plan	Used to describe the Review Plan.
Technical Report	Used to document interim results and status.
Document Review Comment Form	Used to provide comments on reviewed documents.
Tailored Comment Form with Developer Response	Used to provide tailored comments on reviewed documents, and secure a developer response.
Memorandum of Record	Used to meeting minutes, comments, and status reports, or to highlight a significant issue or milestone.
Review Report	Used to document findings and observations.
Feasibility Assessment Report	Used to prepare a detailed analysis of the IV&V Team's assessment of the alternatives.
Requirements Verification Matrix	Used to document the verification criterion that confirms that the system requirements are in accordance with identified IV&V standards.
Anomaly Report Form	Used to document anomalies detected by the IV&V Team.
Test Procedure/Use Case	Used for preparing independent test suites.
Test Report & Requirements Disposition	Used to document monitoring of formal testing.

Template Name	Template Description
Alternate Test Report Outline	Used to provide an alternate test report outline.
Special Studies Report	Used to report on technical, cost, and schedule trade-off analyses related to system development (for example, changes in standards or technology).
IV&V End of Phase Summary Report	Used to provide summary documentation for large system development efforts.
Production Readiness Review Recommendation	Used to generate a report that lists the outstanding issues, relevant risks, recommendations, contingencies, and signatures. This can be presented in memo form with the fields outlined in the template.
IV&V Final Report	Used to issue a report at the end of the System Development Phase or at the conclusion of the IV&V effort.
Sample Progress Report	Used to provide a summary of all IV&V activities performed for the program.
Weekly Status Report	Used to provide weekly status on IV&V activities.
Monthly Status Report	Used to provide monthly status on IV&V activities.
Issue Log	Used to monitor issues on a weekly basis.
Risk Watch List	Used to monitor risks on a bi-weekly basis.
Trip Report	Used to provide summary information on trips taken by IV&V personnel in support of IV&V activities.
IV&V Metrics Report	Used in reporting metrics performance on a monthly basis.
Funds Expended Report	Used to provide an analysis of the IV&V budget.
Contractor Roster/Security Roster	Used to provide information on project staff.
Executive Level Briefing Memorandum	Used to provide key information on development projects.
Lessons Learned Template	Used to provide lessons learned upon the conclusion of In Process Reviews.

Walkthrough Meeting Notice

WALKTHROUGH MEETING NOTICE	
Product/IV&V Control Number:	Walkthrough Number:
Author(s):	Date: Time: Place:
Reason for Walkthrough: <ul style="list-style-type: none"> <input type="checkbox"/> New Development <input type="checkbox"/> Change in Response to Problem Report <input type="checkbox"/> Other (Specify): _____ <input type="checkbox"/> Cross Referenced to: _____ 	
Review Team: Moderator:	Moderator: Indicate who is present; note substitutes; mark-ups.
<p>Note: If you are unable to attend the walkthrough, please review the handout materials and if you have any comments return them to the moderator prior to the walkthrough so they can be considered.</p>	
Walkthrough Disposition: <ul style="list-style-type: none"> <input type="checkbox"/> Accepted <input type="checkbox"/> Accepted With Modifications <input type="checkbox"/> Not Accepted (Explain): _____ 	
Effort Expended:	
Moderator's Signature:	Date:

Defect/Issue List

DEFECT/ISSUE LIST			
Date of Review:			
Walkthrough Number:			
Issue Number	Defect Category (1-8)	Resolution	Comment (Include Reviewer Initials)
		<input type="checkbox"/> Resolved <input type="checkbox"/> Verified	
		<input type="checkbox"/> Resolved <input type="checkbox"/> Verified	
		<input type="checkbox"/> Resolved <input type="checkbox"/> Verified	
		<input type="checkbox"/> Resolved <input type="checkbox"/> Verified	
		<input type="checkbox"/> Resolved <input type="checkbox"/> Verified	

Category

- | | |
|---|---|
| 1. Comment requires immediate resolution. | 5. Comment has been resolved with developer. |
| 2. Comment requires resolution to meet exit criteria. | 6. Comment discussed with developer/still open. |
| 3. Design quality or style suggestion. | 7. Recommendation for future improvement. |
| 4. Question about the document. | 8. Typo, spelling, or minor wording changes. |

Walkthrough Disposition, IV&V Plan

WALKTHROUGH DISPOSITION				
Walkthrough Defect/Issue	Walkthrough Disposition			
	Accepted		Accepted With Modifications	
	Yes	No	Yes	No
Critical Defect(s) Recorded	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Minor Defect(s) Recorded	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Issue(s) Recorded	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

IV&V Plan	
Target system profile:	
IV&V schedule:	
IV&V Team organization:	
Scope of the IV&V effort: Approach Activities Tailoring	

Review Plan

REVIEW PLAN	
REVIEW SUBJECT/OBJECTIVE:	PROJECT:
	PREPARED ON (Date):
	PREPARED BY:
	REVIEWED BY:
	APPROVED BY:
GENERAL REVIEW INFORMATION	
REVIEWED ORGANIZATION:	REVIEW DATE(S):
REVIEWER(S):	REVIEWED GROUP REPRESENTATIVE(S):
RESOURCE REQUIREMENTS:	
REVIEW REFERENCES:	
REVIEW INSTRUCTIONS:	
1. Instruction: Method:	
2. Instruction: Method:	

Technical Report

Technical Report
<p>Technical reports will be utilized to report on all formal concept, requirements, and design reviews. Technical reports will be utilized to report on test readiness reviews by providing recommendations relative to the start of testing. The IV&V Team will also provide a technical report relating to Production (Operational) Readiness Review and Post Implementation Review.</p> <p>Technical reports should be tailored based on the activity and may take the form of a Memorandum of Record (MOR) or simply a formal email.</p>
List the evaluation participants and objective(s).
Detailed Results and Findings.
Detail the extent, cause, impacts, and frequency of any problems or negative trends detected.
Provide appropriate corrective action and/or preventive measure recommendations.

Memorandum of Record (MOR)

Memorandum of Record (MOR)			
General Information			
From:		Date:	
To:		Project No.:	
Document:			
Type of Memo:			
<input type="checkbox"/>	Customer Satisfaction	<input type="checkbox"/>	Inspection/Test Results
<input type="checkbox"/>	Design Review	<input type="checkbox"/>	Process Action Team
<input type="checkbox"/>	Other – IV & V /QA		
Comments:			
Cmt #1			
Cmt #2			
Cmt #3			
<p>The following applicable categories include: (1) comment requires immediate resolution, (2) comment requires resolution to meet exit criteria, (3) design quality or style suggestion, (4) questions about the document, (5) comment has been resolved with developer, (6) comment discussed with developer/still open, (7) recommendations for future improvement, and (8) typo, spelling, or minor word changes.</p>			
Distribution:			
1.		2.	
3.		4.	

Review Report

REVIEW REPORT	
REVIEW INCLUSIVE DATES:	REVIEWERS:
TOTAL EFFORT IN HOURS: Preparation () + Review () + Report () = (). (optional)	
NARRATIVE:	
MAJOR FINDINGS:	
MINOR FINDINGS:	
OBSERVATIONS:	
REVIEWER SIGNATURES:	

Feasibility Assessment Report

FEASIBILITY ASSESSMENT REPORT
Assessment methodology:
Alternatives with accompanying analysis:
Ranking of alternatives:
Recommendations with rationale:
Risks that accompany the recommendations and alternatives:

Anomaly Report Form

Anomaly Report Form			
Incident Number:		Incident Priority:	
Reported By:		Date Reported:	
Application:			
Script No:		Cycle No:	
Testing Phase:			
Incident Response:			
Brief Description:			
Long Description:			
Assigned to:		Date Assigned:	
Resolution:			
Resolved By:		Date Resolved:	
Retested by:		Date Retested:	
Approved By:		Date Approved:	

Test Report & Requirements Disposition

Executive Summary - A short, high-level synopsis of the test activity; include the location(s); relevant dates; major groups who participated; and an overall conclusion of how successful the testing was in meeting the overall objectives.

Test Activities - Describe the results of the preparation activity; an overview of the test activity; and include a statement summarizing the results obtained.

Requirements Table - A table showing the disposition of the requirements as follows.

Test Report & Requirements Disposition					
Functional Area*	Satisfied	Not Tested	Not Satisfied	Total	% Satisfied
Total					

* Functional Area designations included in this table are used for reference only. Functional Area is dependent upon the actual test activity and the specific requirements that are to be validated.

Test Analysis - Summarize the results of the requirements testing; any significant problems encountered and their cause(s), if known; solutions which were incorporated; action plans agreed to; proposed recommendations; an overall conclusion on the level of accomplishment of the core test objectives; and any additional observations on how the testing was conducted.

Lessons Learned - This section of the report may include both positive and negative lessons learned during the test effort. Positive lessons learned will be written in enough detail to provide a clear understanding of the immediate and the long term benefits realized by the program and also clearly describe how this was achieved so it will be easily understood and adopted for future use. For problems encountered, include a statement of the deficiency; cause, if determined; action(s) taken or planned; and a recommendation to prevent future occurrences.

Alternative Test Report Outline

ALTERNATE TEST REPORT OUTLINE

1. Overview
2. Test Summary (for each type of test)
 - Description
 - Issues

Special Studies Report, IV&V End of Phase Summary Report

Special Studies Report
1.0 Purpose and Objectives
2.0 Approach
3.0 Summary of Results

IV&V End of Phase Summary Report
Description of IV&V Tasks Performed
Assessment of Overall System/Software Quality
Recommendations to Proceed to Next Phase
Lessons Learned

Production Readiness Review Recommendation (PRR)

Production Readiness Review Recommendations (PRR)		
Summary:		
List of Outstanding Issues:		
Risks Relevant to PRR:		
Recommendation for PRR:		
All contingencies that impact the recommendation:		
Lessons Learned		
Signature	Title	Date

IV&V Final Report

IV&V FINAL REPORT
1.0 INTRODUCTION
2.0 STANDARDS AND PROCEDURES
3.0 SUMMARY OF LIFECYCLE IV&V TASKS
4.0 LESSONS LEARNED
4.1 SUMMARY OF IV&V PROJECT LESSONS LEARNED AND RECOMMENDATIONS
4.1.1 Product Issues
4.1.2 Process Issues
4.2 DETAILED LESSONS LEARNED
4.2.1 Lessons Learned (Processes to be corrected)
4.2.1.1 Product Issues
Issue:
Recommendation:
4.2.1.2 Process Issues
Issue:
Recommendation:
4.2.2 Positive Lessons Learned (Processes to be maintained)

Sample Progress Report

Sample Progress Report			
Project Name:			
IV&V Program Manager/ Phone:			
Reporting Period:			
Executive Summary			
Deliverable and Meeting Status			
Deliverable	Planned Delivery	Actual Delivery	Status As of End of Period
Meeting/Phonecon	Date	Comments	
Problems/Concerns/Risks			
1.			
2.			
3.			
4.			
5.			
6.			
7.			

IV&V Weekly Status Report

IV&V Weekly Status Report				
Contract: [Insert contract number] Period Ending: [Insert Month, Date, Year]				
CURRENT PERIOD			NEXT PERIOD	
1. MAJOR ACCOMPLISHMENTS/ISSUES			2. SCHEDULED TASKS	
1.	Test Support	•	Next Steps	•
2.	Document Reviews	•	Next Steps	•
3.	Operational Support	•	Next Steps	•
4.	Miscellaneous Activities	•	Next Steps	•
3. MEETINGS & COMMUNICATIONS			4. UPCOMING MEETINGS & COMMUNICATIONS	
1.			1.	
2.			2.	
3.			3.	

Monthly Status Report

[*reflect current date*]

U.S. Department of Education
Federal Student Aid
Union Center Plaza
830 First Street, NE
Washington, DC 20202

Reference: Contract Number: [*insert contract number*]

Subject: Report for [*reflect reporting period*]

[*insert contact*]:

In accordance with the referenced work order, [*insert contractor name*] is submitting the Project Monthly Status Report for [*reflect reporting period*]. If you have any questions, please call [*insert project manager name and contact information*].

Thank you,

[*insert project manager name*]
Project Manager/ [*Insert title*]

cc: [*insert if applicable*]



START HERE
GO FURTHER
FEDERAL STUDENT AID

**Department of Education
Federal Student Aid
[insert Project Name]
IV&V Monthly Status Report – [reflect current reporting
period]**

Prepared for

**Department of Education
Federal Student Aid
Union Center Plaza
830 First Street, NE
Washington, DC 20202**

Prepared by

*[insert contractor name]
[insert contractor address]
[insert contractor city, state, zip]*

Released: *[reflect current date]*

FOREWORD

The [reflect current reporting period] Monthly Status Report for Federal Student Aid [*insert project*] Independent Verification and Validation (IV&V) Program is submitted under Contract [*insert number*] and summarizes the program activities completed, or in process, for the period of [reflect current reporting period]. Specifically, the report details the activities, deliverables, issues, and risks for the period. The report is organized into four major sections as follows:

- **Section 1** – Summary of IV&V Activities for [*reflect current reporting period*]
- **Section 2** – Summary of IV&V Deliverables for [*reflect current reporting period*]
- **Section 3** – Issue Log and Risk Watch List
- **Section 4** – Cumulative IV&V Deliverables Report

Within Section One, there is a summary of [reflect current reporting period] IV&V activities in support of [*insert project name*], including a summary of each of the task areas. Section Two of the report presents the major monthly deliverables. Section Three provides issues and risks for the project. Section Four contains a cumulative list of the IV&V deliverables since project inception.

1.0 SECTION ONE - SUMMARY OF ACTIVITIES FOR [*reflect current reporting period*] - This section contains an overall summary of all activities for the reporting period.

1.1 Summary of IV&V Activities - All activities pertaining to development are highlighted in this section.

1.2 Major Planned Activities for Next Reporting Period - Upcoming activities for the next reporting period are identified in this section.

2.0 SECTION TWO – IV&V DELIVERABLES FOR [reflect current reporting period]

This section contains all major deliverables for the reporting period.

DELIVERABLE	DOCUMENT ID	COMMENTS

3.0 SECTION THREE – ISSUE LOG AND RISK WATCH LIST FOR [reflect current reporting period]

3.1 Issue Log - Summary

[Federal Student Aid Project] IV&V Issue Log [Contractor Name]																		
		NEW ISSUES: CURRENT MONTH			CLOSED ISSUES: CURRENT MONTH				CUMULATIVE TOTAL									
Month	# of Total New Issues	High	Medium	Low	# of Total Closed Issues	High	Medium	Low	Open	Closed								
Total Open Issues as of [Month Year] <table border="1" style="margin: auto;"> <thead> <tr> <th>Total</th> <th>High</th> <th>Medium</th> <th>Low</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>											Total	High	Medium	Low				
Total	High	Medium	Low															

3.2 Issue Log - Details

[Federal Student Aid Project] IV&V Issue Log Open Issues (MM-YY) [Contractor Name]						
ID #	Date	Issue Description	Priority	Sort Code	Status	IV&V Resolution/Comment

3.3 Risk Watch List - Summary

[Federal Student Aid Project] IV&V Risk Watch List [Contractor Name]																		
	NEW RISKS: CURRENT MONTH				CLOSED RISKS: CURRENT MONTH				CUMULATIVE TOTAL									
Month	# of Total New Risks	High	Medium	Low	# of Total Closed Risks	High	Medium	Low	Open	Closed								
Total Open Risks as of [Month Year]																		
<table border="1"> <thead> <tr> <th>Total</th> <th>High</th> <th>Medium</th> <th>Low</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>											Total	High	Medium	Low				
Total	High	Medium	Low															

3.4 Risk Watch List - Details

[Federal Student Aid Project] IV&V Risk Watch List Open Risks (MM-YY) [Contractor Name]									
ID #	Date	Risk	P	I	Risk Exposure	First Indicator	IV&V Risk Mitigation Approach	Status	Condition

4.0 SECTION FOUR – CUMULATIVE IV&V DELIVERABLES

This section highlights all deliverables for the current reporting year.

DELIVERABLE	DOCUMENT ID	COMMENTS (AS NECESSARY)

Issue Log

Issue Log - Summary

[Federal Student Aid Project] IV&V Issue Log [Contractor Name]										
	NEW ISSUES: CURRENT MONTH				CLOSED ISSUES: CURRENT MONTH				CUMULATIVE TOTAL	
Month	# of Total New Issues	High	Medium	Low	# of Total Closed Issues	High	Medium	Low	Open	Closed
Total Open Issues as of [Month Year]										
	Total	High	Medium	Low						

Issue Log - Details

[Federal Student Aid Project] IV&V Issue Log Open Issues (MM-YY) [Contractor Name]						
ID #	Date	Issue Description	Priority	Sort Code	Status	IV&V Resolution/Comment

Risk Watch List

Risk Watch List - Summary

[Federal Student Aid Project] IV&V Risk Watch List [Contractor Name]																		
	NEW RISKS: CURRENT MONTH				CLOSED RISKS: CURRENT MONTH				CUMULATIVE TOTAL									
Month	# of Total New Risks	High	Medium	Low	# of Total Closed Risks	High	Medium	Low	Open	Closed								
Total Open Risks as of [Month Year]																		
<table border="1" style="margin: auto; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="text-align: center;">Total</th> <th style="text-align: center;">High</th> <th style="text-align: center;">Medium</th> <th style="text-align: center;">Low</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>											Total	High	Medium	Low				
Total	High	Medium	Low															

Risk Watch List - Details

[Federal Student Aid Project] IV&V Risk Watch List Open Risks (MM-YY) [Contractor Name]									
ID #	Date	Risk	P	I	Risk Exposure	First Indicator	IV&V Risk Mitigation Approach	Status	Condition

Trip Report

Trip Report
Name of Person(s) traveling:
Dates of travel:
Location of trip:
Purpose of trip:
Summary of Trip:
Findings:
Actions/Issues From Trip: 1. 2.
Lessons Learned (if applicable): 1. 2.

IV&V Metrics Report

START HERE
GO FURTHER
FEDERAL STUDENT AID

**Department of Education
Federal Student Aid
[insert project name]
IV&V Metrics Report
For *[Month Year]***

Prepared for

**Department of Education
Federal Student Aid
Union Center Plaza
830 First Street, NE
Washington, DC 20202**

Prepared by

[insert contractor name]
[insert contractor address]
[insert contractor city, state, zip]

Released: *[Date of Release]*

- 1.0 Introduction**
- 1.1 Methodology**
- 1.2 Summary of IV&V Accomplishments**
 - 1.2.1 Ongoing Activities
 - 1.2.2 New Activities
- 2.0 Assessed [Reporting Month] Deliverables**
- 3.0 Defect Categories**

Category	LCM Stage Metric Category Definition
Vision	
V1	Major impact to critical aspects of the defined system vision, requiring immediate resolution to vision products or processes.
V2	Moderate impact to defined system vision, requiring a resolution to vision products or processes by the next scheduled review cycle.
V3	Minor impact to defined system vision, requiring a resolution to vision products or processes by the next scheduled formal review task.
Definition - Requirement	
DR1	Major defect in defined requirements that either fail to meet an organization's stated critical business needs, or the requirement statement is not constructed to meet industry standards. Both situations require immediate resolution.
DR2	Moderate defect in defined requirements that either fail to meet an organization's stated business needs, or the requirement statement is not constructed to meet industry standards. Both situations require resolution by the next requirements review session.
DR3	Minor defect in defined requirements that require a resolution before final requirements acceptance.
Definition - Design	
DD1	Major impact to system design, which fails to meet critical aspects of a system requirement, requiring immediate resolution.
DD2	Moderate impact to system design, that either partially fulfills a requirement or fails to address aspects of a system requirement, and requires a resolution by the next scheduled update of the design documentation.
DD3	Minor impact to system design that requires a resolution by next design phase or delivery of final design documentation.
Definition - General	
DG1	Major discrepancies occurring within the Definition phase, not related to either a requirement or design issue, requiring immediate resolution.
DG2	Moderate discrepancies occurring within the Definition phase, not related to either a requirement or design issue, that require a resolution by the next scheduled update task.
DG3	Minor discrepancies occurring within the Definition phase, not related to either a requirement or design issue, which require a resolution by the next design phase of delivery of final

Category	LCM Stage Metric Category Definition
	requirements / design documentation.
Construction & Validation (Build / Acquisition)	
CVBA1	Major impact to build / acquisition of proposed solution (developed code, acquired COTS), not meeting critical aspects of system requirements or design, requiring immediate resolution.
CVBA2	Moderate impact to build / acquisition of proposed solution (developed code, acquired COTS), not meeting aspects of system requirements or design, and that requires a resolution within the next scheduled task or walkthrough.
CVBA3	Minor impact to build / acquisition of proposed solution (developed code, acquired COTS), that requires a resolution by next major project phase (or delivery of final system solution).
Construction & Validation (Test)	
CVT1	Major discrepancies within proposed system testing solutions that do not meet critical aspects of system requirements, design, or quality standards for respective test artifact, and require immediate resolution.
CVT2	Moderate discrepancies within proposed system-testing solutions that only partially fulfill aspects of system requirements, design, or quality standards for respective test artifact, and that require a resolution by the next scheduled modifications to test products or processes.
CVT3	Minor discrepancies within proposed system testing solutions, which require a resolution by the next major (or final) system modifications to test products or processes.
Construction & Validation (General)	
CVG1	Major discrepancies occurring within the Construction and Validation phase, not related specifically to a system's proposed build and testing solution, and requiring immediate resolution.
CVG2	Moderate discrepancies occurring within the Construction and Validation phase, not related specifically to a system's proposed build and testing solution, which require a resolution by the next scheduled review task.
CVG3	Minor discrepancies occurring within the Construction and Validation phase, not related specifically to a system's proposed build and testing solution, which require a resolution by acceptance of the final system.
Implementation	
I1	Major discrepancies with the planned and actual implementation of the system, not meeting critical aspects of defined implementation processes and products, requiring immediate resolution.
I2	Moderate discrepancies with the planned and actual implementation of the system, not meeting aspects of defined implementation processes and products, that require a resolution within a specific time period (14 days or less) defined by the customer.
I3	Minor discrepancies with the planned and actual implementation of the system, that require a resolution within a specific time period (15 to 45 days) defined by the customer.

Category	LCM Stage Metric Category Definition
Support & Improvement	
S1	Major discrepancies with the planned and actual support of the implemented system, not meeting critical aspects of defined support products and procedures, requiring immediate resolution.
S2	Moderate discrepancies with the planned and actual support of the implemented system, requiring a resolution within a specific time period (30 days or less) defined by the customer.
S3	Minor discrepancies with the planned support of the implemented system, requiring a resolution within a specific time period (31 to 60 days) defined by the customer.
Retirement	
R1	Major discrepancies within the planned and actual retirement of the system, not meeting critical aspects of defined system retirement processes and products, requiring immediate resolution.
R2	Moderate discrepancies within the planned retirement of the system, not meeting aspects of defined system retirement processes and procedures, requiring a resolution within a specific time period (60 days or less) defined by the customer.
R3	Minor discrepancies within the planned retirement of the system, requiring a resolution within a specific time period (61 to 120 days) defined by the customer.

For consistency, all assigned metric values with a “1” represent a **major** impact or discrepancy, a “2” represent a **moderate** impact or discrepancy, and a “3” represent a **minor** impact or discrepancy.

4.0 Issues and Findings Count

[Reporting Month Year] by Assigned Metric Categories

Deliverable	Assigned Metric Categories							
TOTALS								

Total Number of Issues for [Reporting Month Year]:

Breaking down the [Reporting Month] metric numbers into major impact / deficiency (assigned metric value of “1”), moderate impact / deficiency (assigned metric value of “2”), and minor impact / deficiency (assigned metric value of “3”), the following percentages were derived:

	Total	Percentage
Major impact / deficiency:		
Moderate impact / deficiency:		
Minor impact / deficiency:		
TOTALS		

The following report provides a view of the IV&V metrics for each task area by the lifecycle phase, for [Reporting Month Year].

[Reporting Month Year] IV&V Review by Task Area

Task Area	Definition			Construction & Validation			Implementation			Support & Improvement		
	Maj	Mod	Min	Maj	Mod	Min	Maj	Mod	Min	Maj	Mod	Min
01 – [insert sample task]												
02 – [insert sample task]												
03 – [insert sample task]												
TOTALS												

Funds Expended Report

Project Name					
Funding Projections					
Contract Number:		Order Number:		Period of Performance:	
		Budgeted	Actual and Revised Budget	Remaining Funds (Funded amount -budgeted/actual remaining funds)	COMMENTS
CLIN 0001 - LABOR					
Current Funding as of X Date:					
MM-YY					
Total CLIN 001 Labor					
CLIN 0001 - OTHER DIRECT COSTS (TRAVEL)					
AWARDED AMOUNT AS OF X DATE :					
General Comments					
CLIN 0001 - TOTAL					
MM-YY					
Total					

Contractor Roster/Security Roster

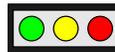
[Vendor Name] Project Contractor / Security Roster (Deliverable #1) For Federal Student Aid – [Program Name] – [Task Identification / Name]						
Vendor Staff Member		Labor Category	IV&V / or Security Task	Title	Security Clearance & Status	ED ID Badge (Y/N) and UCP Desk #
[Contractor Name] [Phone Number]	[E-mail address]	[Labor Category]	[Identify Task]	[Title]	[Clearance] [Status]	[Y/N] [Location Or Not At UCP]
[Contractor Name] [Phone Number]	[E-mail address]	[Labor Category]	[Identify Task]	[Title]	[Clearance] [Status]	[Y/N] [Location Or Not At UCP]
[Contractor Name] [Phone Number]	[E-mail address]	[Labor Category]	[Identify Task]	[Title]	[Clearance] [Status]	[Y/N] [Location Or Not At UCP]
[Contractor Name] [Phone Number]	[E-mail address]	[Labor Category]	[Identify Task]	[Title]	[Clearance] [Status]	[Y/N] [Location Or Not At UCP]

IV&V Executive Briefing Memorandum

Project Summary

- Project Name: *[Insert Project Name.]*
- Project Description: *[Describe the business functionality that the project will enhance/change. Technical information may also be discussed, but the primary focus should be business changes.]*
- Project Dependencies: *[Describe major project dependencies at a high level.]*
- LCM Stage: *[Insert the LCM Stage that the project is currently in.]*
- Next Major Review: *[Describe the next major review that is upcoming for the project, such as Stage Gate Review, SDR, PRR, etc.]*
- IV&V Point of Contact: *[Name of IV&V Project Manager.]*

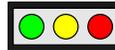
Schedule



[List the top three issues that are impacting the project's schedule and provide IV&V analysis on these issues. The list should be in bulleted form and each issue should be about a paragraph.]

- Issue #1
- Issue #2
- Issue #3

Cost



[List the top three issues that are impacting the project's cost and provide IV&V analysis on these issues. The list should be in bulleted form and each issue should be about a paragraph.]

- Issue #1
- Issue #2
- Issue #3

Performance

[List the top three issues that are impacting the project's performance and provide IV&V analysis on these issues. The list should be in bulleted form and each issue should be about a paragraph. The performance category includes issues related to scope of the project, (i.e. scope creep or scope shrinkage of a phase or the entire project) as well as how the development team is technically executing performance of work on the scope of the project.]

- Issue #1
- Issue #2
- Issue #3

Contracts

[List the top three issues that are impacting the project's contracts and provide IV&V analysis on these issues. The list should be in bulleted form and each issue should be about a paragraph. This section may include issues that arise from contract decisions impacting the work on the project (i.e. funding based on throughput rather than based on achieving development milestones).]

- Issue #1
- Issue #2
- Issue #3

Note: It is understood that IV&V may have limited insight into some areas requested in this memo, particularly the cost and contracts sections. If IV&V does not have information, simply indicate that there is nothing to report for that category. IV&V Managers should endeavor to provide as much information as possible; however they should not seek out new information in the cost or contracts areas beyond the information that has been obtained through other IV&V activities. This memo serves as the overall IV&V view of the project and will be cross-referenced by Federal Student Aid staff with information from the Project Management Office to be used as a tool by Federal Student Aid staff to create a holistic enterprise view of the project.

Legend

- Red Light - Indicates a critical issue that will impact the ability to complete the project
- Yellow Light - Indicates a medium concern that requires watching and possibly more oversight
- Green Light - Indicates that there are no significant issues and the project is on track

Lessons Learned Template

Project Lessons Learned Input Form	1.02
<p>Notes:</p> <ul style="list-style-type: none"> • Read the Project Lessons Learned Input Form Instructions, prior to using this form. • Return completed forms to John Olumoya at John.Olumoya@ed.gov. • To navigate between fields, use the tab key. The template will only allow you to enter data in the grey fields. 	

Project Information		
<i>* = required field</i>	<i>Click F1 for help</i>	
<i>c = combo field</i>		
1. Enter Project Name *		
Only complete this section for new projects or to enter project revisions.		
2. Project Contact		
3. System Name		
4. System Version		
5. Technology (primary) <i>c</i>		
6. Type of Project <i>c*</i>		
7. Project Start (fiscal year) <i>c*</i>		
8. Project Finish (fiscal year, estimated) <i>c*</i>		
9. Estimated Duration (months)		
10. Project Budget Estimate (enter numbers only)	\$	

Stage Information		
<i>* = required field</i>	<i>Click F1 for help</i>	
<i>c = combo field</i>		
1. LCM Stage Name *	Other	
Only complete this section for new stages or to enter stage revisions.		
2. Stage Budget (enter numbers only)		
3. Stage Budge Status <i>c</i>		
4. Stage Contractor/ Vendor Name *		
5. Stage Government COR*		
6. Stage Government PM*		
7. Stage QA/IV&V		
8. Schedule Status <i>c</i>		

<i>Lesson Learned #1</i> * = required field c = combo field	<i>Click F1 for help</i>
1. Lesson Title *	
2. Lesson Background *	
3. Lesson Description *	
4. Is this lesson of high importance? *	
5. Is this lesson sensitive?*	
6. Lesson Type c*	
7. Lesson Category c *	
8. Lesson Sub-Category (i.e. Regression Testing, etc.)	
9. Source Organization *	
10. Source Author *	
11. Origination Date (i.e. 09/20/2007)	

Additional Lessons Learned sections can be added as necessary.

<i>For Administrator Use Only</i>	
Project ID	For Administrator use only
Stage ID	For Administrator use only
Version	1.02
Input Form Type	Project

Appendix F - Security Assessment Questionnaire
(This section is “for example” only)

FOR EXAMPLE ONLY

Appendix F: Security Assessment Questionnaire

System Name:				
System Title:				
System Unique Identifier:				
Major Application:		General Support System:		
<i>Name of Assessors:</i>				
Date of Assessment:				
List of Connected Systems:				
Name of System		Are boundary controls effective?	Certification / Accreditation Date	Planned action if not effective
1.				
2.				
3.				
Security Objectives		FIPS 199 Impact Level (High, Moderate, or Low)		
<i>Confidentiality</i>				
<i>Integrity</i>				

FOR EXAMPLE ONLY

<i>Availability</i>	
<i>FIPS 199 Impact Level (based on highest value of security objective impact level):</i>	
<i>Purpose and Objective of Assessment:</i>	

FOR EXAMPLE ONLY

1. Access Control

Class: Technical

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must limit: (i) information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems); and (ii) the types of transactions and functions that authorized users are permitted to exercise.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AC-1 Access Control Policy and Procedures <table border="1"> <tr> <td>LOW AC-1</td> <td>MOD AC-1</td> <td>HIGH AC-1</td> </tr> </table>	LOW AC-1	MOD AC-1	HIGH AC-1								
LOW AC-1	MOD AC-1	HIGH AC-1									
AC-2 Account Management <table border="1"> <tr> <td>LOW AC-2</td> <td>MOD AC-2 (1) (2) (3) (4)</td> <td>HIGH AC-2 (1) (2) (3) (4)</td> </tr> </table>	LOW AC-2	MOD AC-2 (1) (2) (3) (4)	HIGH AC-2 (1) (2) (3) (4)								
LOW AC-2	MOD AC-2 (1) (2) (3) (4)	HIGH AC-2 (1) (2) (3) (4)									
AC-3 Access Enforcement <table border="1"> <tr> <td>LOW AC-3</td> <td>MOD AC-3 (1)</td> <td>HIGH AC-3 (1)</td> </tr> </table>	LOW AC-3	MOD AC-3 (1)	HIGH AC-3 (1)								
LOW AC-3	MOD AC-3 (1)	HIGH AC-3 (1)									
AC-4 Information Flow Enforcement <table border="1"> <tr> <td>LOW</td> <td>MOD</td> <td>HIGH</td> </tr> </table>	LOW	MOD	HIGH								
LOW	MOD	HIGH									

FOR EXAMPLE ONLY

Security Control			L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
Not Selected	AC-4	AC-4								
AC-5 Separation of Duties										
LOW Not Selected	MOD AC-5	HIGH AC-5								
AC-6 Least Privilege										
LOW Not Selected	MOD AC-6	HIGH AC-6								
AC-7 Unsuccessful Login Attempts										
LOW AC-7	MOD AC-7	HIGH AC-7								
AC-8 System Use Notification										
LOW AC-8	MOD AC-8	HIGH AC-8								

FOR EXAMPLE ONLY

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AC-9 Previous Logon Notification <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected								
LOW Not Selected	MOD Not Selected	HIGH Not Selected									
AC-10 Concurrent Session Control <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH AC-10</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH AC-10								
LOW Not Selected	MOD Not Selected	HIGH AC-10									
AC-11 Session Lock <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD AC-11</td> <td>HIGH AC-11</td> </tr> </table>	LOW Not Selected	MOD AC-11	HIGH AC-11								
LOW Not Selected	MOD AC-11	HIGH AC-11									
AC-12 Session Termination <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD AC-12</td> <td>HIGH AC-12 (1)</td> </tr> </table>	LOW Not Selected	MOD AC-12	HIGH AC-12 (1)								
LOW Not Selected	MOD AC-12	HIGH AC-12 (1)									

FOR EXAMPLE ONLY

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AC-13 Supervision and Review – Access Control <table border="1"> <tr> <td>LOW AC-13</td> <td>MOD AC-13</td> <td>HIGH AC-13 (1)</td> </tr> </table>	LOW AC-13	MOD AC-13	HIGH AC-13 (1)								
LOW AC-13	MOD AC-13	HIGH AC-13 (1)									
AC-14 Permitted Actions without Identification or Authentication <table border="1"> <tr> <td>LOW AC-14</td> <td>MOD AC-14 (1)</td> <td>HIGH AC-14 (1)</td> </tr> </table>	LOW AC-14	MOD AC-14 (1)	HIGH AC-14 (1)								
LOW AC-14	MOD AC-14 (1)	HIGH AC-14 (1)									
AC-15 Automated Marking <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH AC-15</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH AC-15								
LOW Not Selected	MOD Not Selected	HIGH AC-15									
AC-16 Automated Labeling <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected								
LOW Not Selected	MOD Not Selected	HIGH Not Selected									

FOR EXAMPLE ONLY

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AC-17 Remote Access <table border="1"> <tr> <td>LOW AC-17</td> <td>MOD AC-17 (1) (2) (3) (4)</td> <td>HIGH AC-17 (1) (2) (3) (4)</td> </tr> </table>	LOW AC-17	MOD AC-17 (1) (2) (3) (4)	HIGH AC-17 (1) (2) (3) (4)								
LOW AC-17	MOD AC-17 (1) (2) (3) (4)	HIGH AC-17 (1) (2) (3) (4)									
AC-18 Wireless Access Restrictions <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD AC-18 (1)</td> <td>HIGH AC-18 (1) (2)</td> </tr> </table>	LOW Not Selected	MOD AC-18 (1)	HIGH AC-18 (1) (2)								
LOW Not Selected	MOD AC-18 (1)	HIGH AC-18 (1) (2)									
AC-19 Access Control for Portable and Mobile Systems <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD AC-19</td> <td>HIGH AC-19</td> </tr> </table>	LOW Not Selected	MOD AC-19	HIGH AC-19								
LOW Not Selected	MOD AC-19	HIGH AC-19									

FOR EXAMPLE ONLY

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AC-20 Use of External Information Systems <table border="1" data-bbox="121 487 514 581"> <tr> <td>LOW AC-20</td> <td>MOD AC-20 (1)</td> <td>HIGH AC-20 (1)</td> </tr> </table>	LOW AC-20	MOD AC-20 (1)	HIGH AC-20 (1)								
LOW AC-20	MOD AC-20 (1)	HIGH AC-20 (1)									
Effectiveness Level Reached											

NOTES:

FOR EXAMPLE ONLY

2. Awareness and Training

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AT-1 Security Awareness and Training Policy and Procedures <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW AT-1</td> <td style="text-align: center;">MOD AT-1</td> <td style="text-align: center;">HIGH AT-1</td> </tr> </table>	LOW AT-1	MOD AT-1	HIGH AT-1								
LOW AT-1	MOD AT-1	HIGH AT-1									
AT-2 Security Awareness <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW AT-2</td> <td style="text-align: center;">MOD AT-2</td> <td style="text-align: center;">HIGH AT-2</td> </tr> </table>	LOW AT-2	MOD AT-2	HIGH AT-2								
LOW AT-2	MOD AT-2	HIGH AT-2									
AT-3 Security Training <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW AT-3</td> <td style="text-align: center;">MOD AT-3</td> <td style="text-align: center;">HIGH AT-3</td> </tr> </table>	LOW AT-3	MOD AT-3	HIGH AT-3								
LOW AT-3	MOD AT-3	HIGH AT-3									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AT-4 Security Training Records <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW AT-4</td> <td style="text-align: center;">MOD AT-4</td> <td style="text-align: center;">HIGH AT-4</td> </tr> </table>	LOW AT-4	MOD AT-4	HIGH AT-4								
LOW AT-4	MOD AT-4	HIGH AT-4									
AT-5 Contacts with Security Groups and Associations <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW Not Selected</td> <td style="text-align: center;">MOD Not Selected</td> <td style="text-align: center;">HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected								
LOW Not Selected	MOD Not Selected	HIGH Not Selected									
Effectiveness Level Reached											

NOTES:

FOR EXAMPLE ONLY

3. Audit and Accountability

Class: Technical

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AU-1 Audit and Accountability Policy and Procedures <table border="1"> <tr> <td>LOW AU-1</td> <td>MOD AU-1</td> <td>HIGH AU-1</td> </tr> </table>	LOW AU-1	MOD AU-1	HIGH AU-1								
LOW AU-1	MOD AU-1	HIGH AU-1									
AU-2 Auditable Events <table border="1"> <tr> <td>LOW AU-2</td> <td>MOD AU-2 (3)</td> <td>HIGH AUT-2 (1) (2) (3)</td> </tr> </table>	LOW AU-2	MOD AU-2 (3)	HIGH AUT-2 (1) (2) (3)								
LOW AU-2	MOD AU-2 (3)	HIGH AUT-2 (1) (2) (3)									
AU-3 Content of Audit Records <table border="1"> <tr> <td>LOW AU-3</td> <td>MOD AU-3 (1)</td> <td>HIGH AU-3 (1) (2)</td> </tr> </table>	LOW AU-3	MOD AU-3 (1)	HIGH AU-3 (1) (2)								
LOW AU-3	MOD AU-3 (1)	HIGH AU-3 (1) (2)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AU-4 Audit Storage Capacity <table border="1"> <tr> <td>LOW AU-4</td> <td>MOD AU-4</td> <td>HIGH AU-4</td> </tr> </table>	LOW AU-4	MOD AU-4	HIGH AU-4								
LOW AU-4	MOD AU-4	HIGH AU-4									
AU-5 Response to Audit Processing Failures <table border="1"> <tr> <td>LOW AU-5</td> <td>MOD AU-5</td> <td>HIGH AU-5 (1) (2)</td> </tr> </table>	LOW AU-5	MOD AU-5	HIGH AU-5 (1) (2)								
LOW AU-5	MOD AU-5	HIGH AU-5 (1) (2)									
AU-6 Audit Monitoring, Analysis, and Reporting <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD AU-6 (2)</td> <td>HIGH AU-6 (1) (2)</td> </tr> </table>	LOW Not Selected	MOD AU-6 (2)	HIGH AU-6 (1) (2)								
LOW Not Selected	MOD AU-6 (2)	HIGH AU-6 (1) (2)									
AU-7 Audit Reduction and Report Generation <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD AU-7 (1)</td> <td>HIGH AU-7 (1)</td> </tr> </table>	LOW Not Selected	MOD AU-7 (1)	HIGH AU-7 (1)								
LOW Not Selected	MOD AU-7 (1)	HIGH AU-7 (1)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
AU-8 Time Stamps <table border="1"> <tr> <td>LOW AU-8</td> <td>MOD AU-8 (1)</td> <td>HIGH AU-8 (1)</td> </tr> </table>	LOW AU-8	MOD AU-8 (1)	HIGH AU-8 (1)								
LOW AU-8	MOD AU-8 (1)	HIGH AU-8 (1)									
AU-9 Protection of Audit Information <table border="1"> <tr> <td>LOW AU-9</td> <td>MOD AU-9</td> <td>HIGH AU-9</td> </tr> </table>	LOW AU-9	MOD AU-9	HIGH AU-9								
LOW AU-9	MOD AU-9	HIGH AU-9									
AU-10 Non-repudiation <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected								
LOW Not Selected	MOD Not Selected	HIGH Not Selected									
AU-11 Audit Record Retention <table border="1"> <tr> <td>LOW AU-11</td> <td>MOD AU-11</td> <td>HIGH AU-11</td> </tr> </table>	LOW AU-11	MOD AU-11	HIGH AU-11								
LOW AU-11	MOD AU-11	HIGH AU-11									
Effectiveness Level Reached											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied

NOTES:

FOR EXAMPLE ONLY

4. Certification, Accreditation, and Security Assessments

Class: Management

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the security controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the security controls.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures <table border="1"> <tr> <td>LOW CA-1</td> <td>MOD CA-1</td> <td>HIGH CA-1</td> </tr> </table>	LOW CA-1	MOD CA-1	HIGH CA-1								
LOW CA-1	MOD CA-1	HIGH CA-1									
CA-2 Security Assessments <table border="1"> <tr> <td>LOW CA-2</td> <td>MOD CA-2</td> <td>HIGH CA-2</td> </tr> </table>	LOW CA-2	MOD CA-2	HIGH CA-2								
LOW CA-2	MOD CA-2	HIGH CA-2									
CA-3 Information System Connections <table border="1"> <tr> <td>LOW</td> <td>MOD</td> <td>HIGH</td> </tr> </table>	LOW	MOD	HIGH								
LOW	MOD	HIGH									

FOR EXAMPLE ONLY

Security Control			L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
CA-3	CA-3	CA-3								
CA-4 Security Certification										
LOW CA-4	MOD CA-4 (1)	HIGH CA-4 (1)								
CA-5 Plan of Action and Milestones										
LOW CA-5	MOD CA-5	HIGH CA-5								
CA-6 Security Accreditation										
LOW CA-6	MOD CA-6	HIGH CA-6								
CA-7 Continuous Monitoring										
LOW CA-7	MOD CA-7	HIGH CA-7								

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
Effectiveness Level Reached								

NOTES:

FOR EXAMPLE ONLY

5. Configuration Management

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems; (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems; and (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
CM-1 Configuration Management Policy and Procedures <table border="1"> <tr> <td>LOW CM-1</td> <td>MOD CM-1</td> <td>HIGH CM-1</td> </tr> </table>	LOW CM-1	MOD CM-1	HIGH CM-1								
LOW CM-1	MOD CM-1	HIGH CM-1									
CM-2 Baseline Configuration <table border="1"> <tr> <td>LOW CM-2</td> <td>MOD CM-2 (1)</td> <td>HIGH CM-2 (1) (2)</td> </tr> </table>	LOW CM-2	MOD CM-2 (1)	HIGH CM-2 (1) (2)								
LOW CM-2	MOD CM-2 (1)	HIGH CM-2 (1) (2)									
CM-3 Configuration Change Control <table border="1"> <tr> <td>LOW Not</td> <td>MOD CM-3</td> <td>HIGH CM-3</td> </tr> </table>	LOW Not	MOD CM-3	HIGH CM-3								
LOW Not	MOD CM-3	HIGH CM-3									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>Selected</td> <td></td> <td>(1)</td> </tr> </table>	Selected		(1)								
Selected		(1)									
CM-4 Monitoring Configuration Changes <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD CM-4</td> <td>HIGH CM-4</td> </tr> </table>	LOW Not Selected	MOD CM-4	HIGH CM-4								
LOW Not Selected	MOD CM-4	HIGH CM-4									
CM-5 Access Restrictions for Change <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD CM-5</td> <td>HIGH CM-5 (1)</td> </tr> </table>	LOW Not Selected	MOD CM-5	HIGH CM-5 (1)								
LOW Not Selected	MOD CM-5	HIGH CM-5 (1)									
CM-6 Configuration Settings <table border="1"> <tr> <td>LOW CM-6</td> <td>MOD CM-6</td> <td>HIGH CM-6 (1)</td> </tr> </table>	LOW CM-6	MOD CM-6	HIGH CM-6 (1)								
LOW CM-6	MOD CM-6	HIGH CM-6 (1)									
CM-7 Least Functionality <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD CM-7</td> <td>HIGH CM-7 (1)</td> </tr> </table>	LOW Not Selected	MOD CM-7	HIGH CM-7 (1)								
LOW Not Selected	MOD CM-7	HIGH CM-7 (1)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied									
CM-8 Information System Component Inventory <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW</td> <td style="text-align: center;">MOD</td> <td style="text-align: center;">HIGH</td> </tr> <tr> <td style="text-align: center;">CM-8</td> <td style="text-align: center;">CM-8</td> <td style="text-align: center;">CM-8</td> </tr> <tr> <td></td> <td style="text-align: center;">(1)</td> <td style="text-align: center;">(1) (2)</td> </tr> </table>	LOW	MOD	HIGH	CM-8	CM-8	CM-8		(1)	(1) (2)								
LOW	MOD	HIGH															
CM-8	CM-8	CM-8															
	(1)	(1) (2)															
Effectiveness Level Reached																	

NOTES:

FOR EXAMPLE ONLY

6. Contingency Planning

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
CP-1 Contingency Planning Policy and Procedures <table border="1"> <tr> <td>LOW CP-1</td> <td>MOD CP-1</td> <td>HIGH CP-1</td> </tr> </table>	LOW CP-1	MOD CP-1	HIGH CP-1								
LOW CP-1	MOD CP-1	HIGH CP-1									
CP-2 Contingency Plan <table border="1"> <tr> <td>LOW CP-2</td> <td>MOD CP-2 (1)</td> <td>HIGH CP-2 (1) (2)</td> </tr> </table>	LOW CP-2	MOD CP-2 (1)	HIGH CP-2 (1) (2)								
LOW CP-2	MOD CP-2 (1)	HIGH CP-2 (1) (2)									
CP-3 Contingency Training <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD CP-3</td> <td>HIGH CP-3 (1)</td> </tr> </table>	LOW Not Selected	MOD CP-3	HIGH CP-3 (1)								
LOW Not Selected	MOD CP-3	HIGH CP-3 (1)									
CP-4 Contingency Plan Testing											

FOR EXAMPLE ONLY

Security Control and Exercises	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>LOW CP-4</td> <td>MOD CP-4 (1)</td> <td>HIGH CP-4 (1) (2)</td> </tr> </table>	LOW CP-4	MOD CP-4 (1)	HIGH CP-4 (1) (2)								
LOW CP-4	MOD CP-4 (1)	HIGH CP-4 (1) (2)									
CP-5 Contingency Plan Update <table border="1"> <tr> <td>LOW CP-5</td> <td>MOD CP-5</td> <td>HIGH CP-5</td> </tr> </table>	LOW CP-5	MOD CP-5	HIGH CP-5								
LOW CP-5	MOD CP-5	HIGH CP-5									
CP-6 Alternate Storage Site <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD CP-6 (1) (3)</td> <td>HIGH CP-6 (1) (2) (3)</td> </tr> </table>	LOW Not Selected	MOD CP-6 (1) (3)	HIGH CP-6 (1) (2) (3)								
LOW Not Selected	MOD CP-6 (1) (3)	HIGH CP-6 (1) (2) (3)									
CP-7 Alternate Processing Site <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD CP-7 (1) (2) (3)</td> <td>HIGH CP-7 (1) (2) (3) (4)</td> </tr> </table>	LOW Not Selected	MOD CP-7 (1) (2) (3)	HIGH CP-7 (1) (2) (3) (4)								
LOW Not Selected	MOD CP-7 (1) (2) (3)	HIGH CP-7 (1) (2) (3) (4)									
CP-8 Telecommunications Services											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD CP-8 (1) (2)</td> <td>HIGH CP-8 (1) (2) (3) (4)</td> </tr> </table>	LOW Not Selected	MOD CP-8 (1) (2)	HIGH CP-8 (1) (2) (3) (4)								
LOW Not Selected	MOD CP-8 (1) (2)	HIGH CP-8 (1) (2) (3) (4)									
CP-9 Information System Backup <table border="1"> <tr> <td>LOW CP-9</td> <td>MOD CP-9 (1) (4)</td> <td>HIGH CP-9 (1) (2) (3) (4)</td> </tr> </table>	LOW CP-9	MOD CP-9 (1) (4)	HIGH CP-9 (1) (2) (3) (4)								
LOW CP-9	MOD CP-9 (1) (4)	HIGH CP-9 (1) (2) (3) (4)									
CP-10 Information System Recovery and Reconstitution <table border="1"> <tr> <td>LOW CP-10</td> <td>MOD CP-10</td> <td>HIGH CP-10 (1)</td> </tr> </table>	LOW CP-10	MOD CP-10	HIGH CP-10 (1)								
LOW CP-10	MOD CP-10	HIGH CP-10 (1)									
Effectiveness Level Reached											

NOTES:

FOR EXAMPLE ONLY

7. Identification and Authentication

Class: Technical

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) identify information system users, processes acting on behalf of users, or devices; and (ii) authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
IA-1 Identification and Authentication Policy and Procedures <table border="1"> <tr> <td>LOW IA-1</td> <td>MOD IA-1</td> <td>HIGH IA-1</td> </tr> </table>	LOW IA-1	MOD IA-1	HIGH IA-1								
LOW IA-1	MOD IA-1	HIGH IA-1									
IA-2 User Identification and Authentication <table border="1"> <tr> <td>LOW IA-2</td> <td>MOD IA-2 (1)</td> <td>HIGH IA-2 (2) (3)</td> </tr> </table>	LOW IA-2	MOD IA-2 (1)	HIGH IA-2 (2) (3)								
LOW IA-2	MOD IA-2 (1)	HIGH IA-2 (2) (3)									
IA-3 Device Identification and Authentication <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD IA-3</td> <td>HIGH IA-3</td> </tr> </table>	LOW Not Selected	MOD IA-3	HIGH IA-3								
LOW Not Selected	MOD IA-3	HIGH IA-3									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
IA-4 Identifier Management <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW IA-4</td> <td style="text-align: center;">MOD IA-4</td> <td style="text-align: center;">HIGH IA-4</td> </tr> </table>	LOW IA-4	MOD IA-4	HIGH IA-4								
LOW IA-4	MOD IA-4	HIGH IA-4									
IA-5 Authenticator Management <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW IA-5</td> <td style="text-align: center;">MOD IA-5</td> <td style="text-align: center;">HIGH IA-5</td> </tr> </table>	LOW IA-5	MOD IA-5	HIGH IA-5								
LOW IA-5	MOD IA-5	HIGH IA-5									
IA-6 Authenticator Feedback <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW IA-6</td> <td style="text-align: center;">MOD IA-6</td> <td style="text-align: center;">HIGH IA-6</td> </tr> </table>	LOW IA-6	MOD IA-6	HIGH IA-6								
LOW IA-6	MOD IA-6	HIGH IA-6									
IA-7 Cryptographic Module Authentication <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW IA-7</td> <td style="text-align: center;">MOD IA-7</td> <td style="text-align: center;">HIGH IA-7</td> </tr> </table>	LOW IA-7	MOD IA-7	HIGH IA-7								
LOW IA-7	MOD IA-7	HIGH IA-7									
Effectiveness Level Reached											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied

NOTES:

FOR EXAMPLE ONLY

8. Incident Response

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) establish an operational incident response capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
IR-1 Incident Response Policy and Procedures <table border="1"> <tr> <td>LOW IR-1</td> <td>MOD IR-1</td> <td>HIGH IR-1</td> </tr> </table>	LOW IR-1	MOD IR-1	HIGH IR-1								
LOW IR-1	MOD IR-1	HIGH IR-1									
IR-2 Incident Response Training <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD IR-2</td> <td>HIGH IR-2 (1)</td> </tr> </table>	LOW Not Selected	MOD IR-2	HIGH IR-2 (1)								
LOW Not Selected	MOD IR-2	HIGH IR-2 (1)									
IR-3 Incident Response Testing and Exercises <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD IR-3</td> <td>HIGH IR-3 (1)</td> </tr> </table>	LOW Not Selected	MOD IR-3	HIGH IR-3 (1)								
LOW Not Selected	MOD IR-3	HIGH IR-3 (1)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
IR-4 Incident Handling <table border="1"> <tr> <td>LOW IR-4</td> <td>MOD IR-4 (1)</td> <td>HIGH IR-4 (1)</td> </tr> </table>	LOW IR-4	MOD IR-4 (1)	HIGH IR-4 (1)								
LOW IR-4	MOD IR-4 (1)	HIGH IR-4 (1)									
IA-5 Incident Monitoring <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD IR-5</td> <td>HIGH IR-5 (1)</td> </tr> </table>	LOW Not Selected	MOD IR-5	HIGH IR-5 (1)								
LOW Not Selected	MOD IR-5	HIGH IR-5 (1)									
IR-6 Incident Reporting <table border="1"> <tr> <td>LOW IR-6</td> <td>MOD IR-6 (1)</td> <td>HIGH IR-6 (1)</td> </tr> </table>	LOW IR-6	MOD IR-6 (1)	HIGH IR-6 (1)								
LOW IR-6	MOD IR-6 (1)	HIGH IR-6 (1)									
IR-7 Incident Response Assistance <table border="1"> <tr> <td>LOW IR-7</td> <td>MOD IR-7 (1)</td> <td>HIGH IR-7 (1)</td> </tr> </table>	LOW IR-7	MOD IR-7 (1)	HIGH IR-7 (1)								
LOW IR-7	MOD IR-7 (1)	HIGH IR-7 (1)									
Effectiveness Level Reached											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied

NOTES:

FOR EXAMPLE ONLY

9. Maintenance

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
MA-1 System Maintenance Policy and Procedures <table border="1"> <tr> <td>LOW MA-1</td> <td>MOD MA-1</td> <td>HIGH MA-1</td> </tr> </table>	LOW MA-1	MOD MA-1	HIGH MA-1								
LOW MA-1	MOD MA-1	HIGH MA-1									
MA-2 Controlled Maintenance <table border="1"> <tr> <td>LOW MA-2</td> <td>MOD MA-2 (1)</td> <td>HIGH MA-2 (1) (2)</td> </tr> </table>	LOW MA-2	MOD MA-2 (1)	HIGH MA-2 (1) (2)								
LOW MA-2	MOD MA-2 (1)	HIGH MA-2 (1) (2)									
MA-3 Maintenance Tools <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD MA-3 (1) (2)</td> <td>HIGH MA-3 (1) (2) (3)</td> </tr> </table>	LOW Not Selected	MOD MA-3 (1) (2)	HIGH MA-3 (1) (2) (3)								
LOW Not Selected	MOD MA-3 (1) (2)	HIGH MA-3 (1) (2) (3)									
MA-4 Remote Maintenance											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>LOW MA-4</td> <td>MOD MA-4</td> <td>HIGH MA-4 (1) (2) (3)</td> </tr> </table>	LOW MA-4	MOD MA-4	HIGH MA-4 (1) (2) (3)								
LOW MA-4	MOD MA-4	HIGH MA-4 (1) (2) (3)									
MA-5 Maintenance Personnel <table border="1"> <tr> <td>LOW MA-5</td> <td>MOD MA-5</td> <td>HIGH MA-5</td> </tr> </table>	LOW MA-5	MOD MA-5	HIGH MA-5								
LOW MA-5	MOD MA-5	HIGH MA-5									
MA-6 Timely Maintenance <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD MA-6</td> <td>HIGH MA-6</td> </tr> </table>	LOW Not Selected	MOD MA-6	HIGH MA-6								
LOW Not Selected	MOD MA-6	HIGH MA-6									
Effectiveness Level Reached											

NOTES:

FOR EXAMPLE ONLY

10. Media Protection

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) protect information contained in organizational information systems in printed form or on digital media; (ii) limit access to information in printed form or on digital media removed from organizational information systems to authorized users; and (iii) sanitize or destroy digital media before disposal or release for reuse.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
MP-1 Media Protection Policy and Procedures <table border="1"> <tr> <td>LOW MP-1</td> <td>MOD MP-1</td> <td>HIGH MP-1</td> </tr> </table>	LOW MP-1	MOD MP-1	HIGH MP-1								
LOW MP-1	MOD MP-1	HIGH MP-1									
MP-2 Media Access <table border="1"> <tr> <td>LOW MP-2</td> <td>MOD MP-2 (1)</td> <td>HIGH MP-2 (1)</td> </tr> </table>	LOW MP-2	MOD MP-2 (1)	HIGH MP-2 (1)								
LOW MP-2	MOD MP-2 (1)	HIGH MP-2 (1)									
MP-3 Media Labeling <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH MP-3</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH MP-3								
LOW Not Selected	MOD Not Selected	HIGH MP-3									
MP-4 Media Storage											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD MP-4</td> <td>HIGH MP-4</td> </tr> </table>	LOW Not Selected	MOD MP-4	HIGH MP-4								
LOW Not Selected	MOD MP-4	HIGH MP-4									
MP-5 Media Transport <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD MP-5 (1) (2)</td> <td>HIGH MP-5 (1) (2) (3)</td> </tr> </table>	LOW Not Selected	MOD MP-5 (1) (2)	HIGH MP-5 (1) (2) (3)								
LOW Not Selected	MOD MP-5 (1) (2)	HIGH MP-5 (1) (2) (3)									
MP-6 Media Sanitization and Disposal <table border="1"> <tr> <td>LOW MP-6</td> <td>MOD MP-6</td> <td>HIGH MP-6 (1) (2)</td> </tr> </table>	LOW MP-6	MOD MP-6	HIGH MP-6 (1) (2)								
LOW MP-6	MOD MP-6	HIGH MP-6 (1) (2)									
Effectiveness Level Reached											

NOTES:

FOR EXAMPLE ONLY

11. Physical and Environmental Protection

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PE-1 Physical and Environmental Protection Policy and Procedures <table border="1"> <tr> <td>LOW PE-1</td> <td>MOD PE-1</td> <td>HIGH PE-1</td> </tr> </table>	LOW PE-1	MOD PE-1	HIGH PE-1								
LOW PE-1	MOD PE-1	HIGH PE-1									
PE-2 Physical Access Authorizations <table border="1"> <tr> <td>LOW PE-2</td> <td>MOD PE-2</td> <td>HIGH PE-2</td> </tr> </table>	LOW PE-2	MOD PE-2	HIGH PE-2								
LOW PE-2	MOD PE-2	HIGH PE-2									
PE-3 Physical Access Control <table border="1"> <tr> <td>LOW PE-3</td> <td>MOD PE-3</td> <td>HIGH PE-3 (1)</td> </tr> </table>	LOW PE-3	MOD PE-3	HIGH PE-3 (1)								
LOW PE-3	MOD PE-3	HIGH PE-3 (1)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PE-4 Access Control for Transmission Medium <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH PE-4</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH PE-4								
LOW Not Selected	MOD Not Selected	HIGH PE-4									
PE-5 Access Control for Display Medium <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD PE-5</td> <td>HIGH PE-5</td> </tr> </table>	LOW Not Selected	MOD PE-5	HIGH PE-5								
LOW Not Selected	MOD PE-5	HIGH PE-5									
PE-6 Monitoring Physical Access <table border="1"> <tr> <td>LOW PE-6</td> <td>MOD PE-6 (1)</td> <td>HIGH PE-6 (1) (2)</td> </tr> </table>	LOW PE-6	MOD PE-6 (1)	HIGH PE-6 (1) (2)								
LOW PE-6	MOD PE-6 (1)	HIGH PE-6 (1) (2)									
PE-7 Visitor Control <table border="1"> <tr> <td>LOW PE-7</td> <td>MOD PE-7 (1)</td> <td>HIGH PE-7 (1)</td> </tr> </table>	LOW PE-7	MOD PE-7 (1)	HIGH PE-7 (1)								
LOW PE-7	MOD PE-7 (1)	HIGH PE-7 (1)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PE-8 Access Records <table border="1"> <tr> <td>LOW PE-8</td> <td>MOD PE-8 (1)</td> <td>HIGH PE-8 (1) (2)</td> </tr> </table>	LOW PE-8	MOD PE-8 (1)	HIGH PE-8 (1) (2)								
LOW PE-8	MOD PE-8 (1)	HIGH PE-8 (1) (2)									
PE-9 Power Equipment and Power Cabling <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD PE-9</td> <td>HIGH PE-9</td> </tr> </table>	LOW Not Selected	MOD PE-9	HIGH PE-9								
LOW Not Selected	MOD PE-9	HIGH PE-9									
PE-10 Emergency Shutoff <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD PE-10</td> <td>HIGH PE-10 (1)</td> </tr> </table>	LOW Not Selected	MOD PE-10	HIGH PE-10 (1)								
LOW Not Selected	MOD PE-10	HIGH PE-10 (1)									
PE-11 Emergency Power <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD PE-11</td> <td>HIGH PE-11 (1)</td> </tr> </table>	LOW Not Selected	MOD PE-11	HIGH PE-11 (1)								
LOW Not Selected	MOD PE-11	HIGH PE-11 (1)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PE-12 Emergency Lighting <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">LOW PE-12</td> <td style="width: 33%; text-align: center;">MOD PE-12</td> <td style="width: 33%; text-align: center;">HIGH PE-12</td> </tr> </table>	LOW PE-12	MOD PE-12	HIGH PE-12								
LOW PE-12	MOD PE-12	HIGH PE-12									
PE-13 Fire Protection <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">LOW PE-13</td> <td style="width: 33%; text-align: center;">MOD PE-13 (1) (2) (3)</td> <td style="width: 33%; text-align: center;">HIGH PE-13 (1) (2) (3)</td> </tr> </table>	LOW PE-13	MOD PE-13 (1) (2) (3)	HIGH PE-13 (1) (2) (3)								
LOW PE-13	MOD PE-13 (1) (2) (3)	HIGH PE-13 (1) (2) (3)									
PE-14 Temperature and Humidity Controls <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">LOW PE-14</td> <td style="width: 33%; text-align: center;">MOD PE-14</td> <td style="width: 33%; text-align: center;">HIGH PE-14</td> </tr> </table>	LOW PE-14	MOD PE-14	HIGH PE-14								
LOW PE-14	MOD PE-14	HIGH PE-14									
PE-15 Water Damage Protection <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">LOW PE-15</td> <td style="width: 33%; text-align: center;">MOD PE-15</td> <td style="width: 33%; text-align: center;">HIGH PE-15 (1)</td> </tr> </table>	LOW PE-15	MOD PE-15	HIGH PE-15 (1)								
LOW PE-15	MOD PE-15	HIGH PE-15 (1)									
PE-16 Delivery and Removal											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>LOW PE-16</td> <td>MOD PE-16</td> <td>HIGH PE-16</td> </tr> </table>	LOW PE-16	MOD PE-16	HIGH PE-16								
LOW PE-16	MOD PE-16	HIGH PE-16									
PE-17 Alternate Work Site <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD PE-17</td> <td>HIGH PE-17</td> </tr> </table>	LOW Not Selected	MOD PE-17	HIGH PE-17								
LOW Not Selected	MOD PE-17	HIGH PE-17									
PE-18 Location of Information System Components <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD PE-18</td> <td>HIGH PE-18 (1)</td> </tr> </table>	LOW Not Selected	MOD PE-18	HIGH PE-18 (1)								
LOW Not Selected	MOD PE-18	HIGH PE-18 (1)									
PE-19 Information Leakage <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected								
LOW Not Selected	MOD Not Selected	HIGH Not Selected									
Effectiveness Level Reached											

FOR EXAMPLE ONLY

NOTES:

FOR EXAMPLE ONLY

12. Planning

Class: Management

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PL-1 Security Planning Policy and Procedures <table border="1"> <tr> <td>LOW PL-1</td> <td>MOD PL-1</td> <td>HIGH PL-1</td> </tr> </table>	LOW PL-1	MOD PL-1	HIGH PL-1								
LOW PL-1	MOD PL-1	HIGH PL-1									
PL-2 System Security Plan <table border="1"> <tr> <td>LOW PL-2</td> <td>MOD PL-2</td> <td>HIGH PL-2</td> </tr> </table>	LOW PL-2	MOD PL-2	HIGH PL-2								
LOW PL-2	MOD PL-2	HIGH PL-2									
PL-3 System Security Plan Update <table border="1"> <tr> <td>LOW PL-3</td> <td>MOD PL-3</td> <td>HIGH PL-3</td> </tr> </table>	LOW PL-3	MOD PL-3	HIGH PL-3								
LOW PL-3	MOD PL-3	HIGH PL-3									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PL-4 Rules of Behavior <table border="1"> <tr> <td>LOW PL-4</td> <td>MOD PL-4</td> <td>HIGH PL-4</td> </tr> </table>	LOW PL-4	MOD PL-4	HIGH PL-4								
LOW PL-4	MOD PL-4	HIGH PL-4									
PL-5 Privacy Impact Assessment <table border="1"> <tr> <td>LOW PL-5</td> <td>MOD PL-5</td> <td>HIGH PL-5</td> </tr> </table>	LOW PL-5	MOD PL-5	HIGH PL-5								
LOW PL-5	MOD PL-5	HIGH PL-5									
PL-6 Security-Related Activity Planning <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD PL-6</td> <td>HIGH PL-6</td> </tr> </table>	LOW Not Selected	MOD PL-6	HIGH PL-6								
LOW Not Selected	MOD PL-6	HIGH PL-6									
Effectiveness Level Reached											

NOTES:

FOR EXAMPLE ONLY

13. Personnel Security

Class: Operational

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PS-1 Personnel Security Policy and Procedures <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW PS-1</td> <td style="text-align: center;">MOD PS-1</td> <td style="text-align: center;">HIGH PS-1</td> </tr> </table>	LOW PS-1	MOD PS-1	HIGH PS-1								
LOW PS-1	MOD PS-1	HIGH PS-1									
PS-2 Position Categorization <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW PS-2</td> <td style="text-align: center;">MOD PS-2</td> <td style="text-align: center;">HIGH PS-2</td> </tr> </table>	LOW PS-2	MOD PS-2	HIGH PS-2								
LOW PS-2	MOD PS-2	HIGH PS-2									
PS-3 Personnel Screening <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW PS-3</td> <td style="text-align: center;">MOD PS-3</td> <td style="text-align: center;">HIGH PS-3</td> </tr> </table>	LOW PS-3	MOD PS-3	HIGH PS-3								
LOW PS-3	MOD PS-3	HIGH PS-3									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
PS-4 Personnel Termination <table border="1"> <tr> <td>LOW PS-4</td> <td>MOD PS-4</td> <td>HIGH PS-4</td> </tr> </table>	LOW PS-4	MOD PS-4	HIGH PS-4								
LOW PS-4	MOD PS-4	HIGH PS-4									
PS-5 Personnel Transfer <table border="1"> <tr> <td>LOW PS-5</td> <td>MOD PS-5</td> <td>HIGH PS-5</td> </tr> </table>	LOW PS-5	MOD PS-5	HIGH PS-5								
LOW PS-5	MOD PS-5	HIGH PS-5									
PS-6 Access Agreements <table border="1"> <tr> <td>LOW PS-6</td> <td>MOD PS-6</td> <td>HIGH PS-6</td> </tr> </table>	LOW PS-6	MOD PS-6	HIGH PS-6								
LOW PS-6	MOD PS-6	HIGH PS-6									
PS-7 Third-Party Personnel Security <table border="1"> <tr> <td>LOW PS-7</td> <td>MOD PS-7</td> <td>HIGH PS-7</td> </tr> </table>	LOW PS-7	MOD PS-7	HIGH PS-7								
LOW PS-7	MOD PS-7	HIGH PS-7									
PS-8 Personnel Sanctions <table border="1"> <tr> <td>LOW</td> <td>MOD</td> <td>HIGH</td> </tr> </table>	LOW	MOD	HIGH								
LOW	MOD	HIGH									

FOR EXAMPLE ONLY

Security Control			L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
PS-8	PS-8	PS-8								
Effectiveness Level Reached										

NOTES:

FOR EXAMPLE ONLY

14. Risk Assessment

Class: Management

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing storage, or transmission of organizational information.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
RA-1 Risk Assessment Policy and Procedures <table border="1"> <tr> <td>LOW RA-1</td> <td>MOD RA-1</td> <td>HIGH RA-1</td> </tr> </table>	LOW RA-1	MOD RA-1	HIGH RA-1								
LOW RA-1	MOD RA-1	HIGH RA-1									
RA-2 Security Categorization <table border="1"> <tr> <td>LOW RA-2</td> <td>MOD RA-2</td> <td>HIGH RA-2</td> </tr> </table>	LOW RA-2	MOD RA-2	HIGH RA-2								
LOW RA-2	MOD RA-2	HIGH RA-2									
RA-3 Risk Assessment <table border="1"> <tr> <td>LOW RA-3</td> <td>MOD RA-3</td> <td>HIGH RA-3</td> </tr> </table>	LOW RA-3	MOD RA-3	HIGH RA-3								
LOW RA-3	MOD RA-3	HIGH RA-3									
RA-4 Risk Assessment Update											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>LOW RA-4</td> <td>MOD RA-4</td> <td>HIGH RA-4</td> </tr> </table>	LOW RA-4	MOD RA-4	HIGH RA-4								
LOW RA-4	MOD RA-4	HIGH RA-4									
RA-5 Vulnerability Scanning <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD RA-5</td> <td>HIGH RA-5 (1) (2)</td> </tr> </table>	LOW Not Selected	MOD RA-5	HIGH RA-5 (1) (2)								
LOW Not Selected	MOD RA-5	HIGH RA-5 (1) (2)									
Effectiveness Level Reached											

NOTES:

FOR EXAMPLE ONLY

15. System and Services Acquisition

Class: Management

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
SA-1 System and Services Acquisition Policy and Procedures <table border="1"> <tr> <td>LOW SA-1</td> <td>MOD SA-1</td> <td>HIGH SA-1</td> </tr> </table>	LOW SA-1	MOD SA-1	HIGH SA-1								
LOW SA-1	MOD SA-1	HIGH SA-1									
SA-2 Allocation of Resources <table border="1"> <tr> <td>LOW SA-2</td> <td>MOD SA-2</td> <td>HIGH SA-2</td> </tr> </table>	LOW SA-2	MOD SA-2	HIGH SA-2								
LOW SA-2	MOD SA-2	HIGH SA-2									
SA-3 Life Cycle Support <table border="1"> <tr> <td>LOW SA-3</td> <td>MOD SA-3</td> <td>HIGH SA-3</td> </tr> </table>	LOW SA-3	MOD SA-3	HIGH SA-3								
LOW SA-3	MOD SA-3	HIGH SA-3									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
SA-4 Acquisitions <table border="1"> <tr> <td>LOW SA-4</td> <td>MOD SA-4 (1)</td> <td>HIGH SA-4 (1)</td> </tr> </table>	LOW SA-4	MOD SA-4 (1)	HIGH SA-4 (1)								
LOW SA-4	MOD SA-4 (1)	HIGH SA-4 (1)									
SA-5 Information System Documentation <table border="1"> <tr> <td>LOW SA-5</td> <td>MOD SA-5 (1)</td> <td>HIGH SA-5 (1) (2)</td> </tr> </table>	LOW SA-5	MOD SA-5 (1)	HIGH SA-5 (1) (2)								
LOW SA-5	MOD SA-5 (1)	HIGH SA-5 (1) (2)									
SA-6 Software Usage Restrictions <table border="1"> <tr> <td>LOW SA-6</td> <td>MOD SA-6</td> <td>HIGH SA-6</td> </tr> </table>	LOW SA-6	MOD SA-6	HIGH SA-6								
LOW SA-6	MOD SA-6	HIGH SA-6									
SA-7 User Installed Software <table border="1"> <tr> <td>LOW SA-7</td> <td>MOD SA-7</td> <td>HIGH SA-7</td> </tr> </table>	LOW SA-7	MOD SA-7	HIGH SA-7								
LOW SA-7	MOD SA-7	HIGH SA-7									
SA-8 Security Design Principles											

FOR EXAMPLE ONLY

Security Control			L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
LOW Not Selected	MOD SA-8	HIGH SA-8								
SA-9 External Information System Services										
LOW SA-9	MOD SA-9	HIGH SA-9								
SA-10 Developer Configuration Management										
LOW Not Selected	MOD Not Selected	HIGH SA-10								
SA-11 Developer Security Training										
LOW Not Selected	MOD SA-11	HIGH SA-11								
Effectiveness Level Reached										

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied

NOTES:

FOR EXAMPLE ONLY

16. System and Communications Protection

Class: Technical

FIPS 199 Impact Level: Low _____ Moderate _____ High _____

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
SC-1 System and Communications Protection Policy and Procedures <table border="1"> <tr> <td>LOW SC-1</td> <td>MOD SC-1</td> <td>HIGH SC-1</td> </tr> </table>	LOW SC-1	MOD SC-1	HIGH SC-1								
LOW SC-1	MOD SC-1	HIGH SC-1									
SC-2 Application Partitioning <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-2</td> <td>HIGH SC-2</td> </tr> </table>	LOW Not Selected	MOD SC-2	HIGH SC-2								
LOW Not Selected	MOD SC-2	HIGH SC-2									
SC-3 Security Function Isolation <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH SC-3</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH SC-3								
LOW Not Selected	MOD Not Selected	HIGH SC-3									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
SC-4 Information Remnance <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-4</td> <td>HIGH SC-4</td> </tr> </table>	LOW Not Selected	MOD SC-4	HIGH SC-4								
LOW Not Selected	MOD SC-4	HIGH SC-4									
SC-5 Denial of Service Protection <table border="1"> <tr> <td>LOW SC-5</td> <td>MOD SC-5</td> <td>HIGH SC-5</td> </tr> </table>	LOW SC-5	MOD SC-5	HIGH SC-5								
LOW SC-5	MOD SC-5	HIGH SC-5									
SC-6 Resource Priority <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected								
LOW Not Selected	MOD Not Selected	HIGH Not Selected									
SC-7 Boundary Protection <table border="1"> <tr> <td>LOW SC-7</td> <td>MOD SC-7 (1) (2) (3) (4) (5)</td> <td>HIGH SC-7 (1) (2) (3) (4) (5) (6)</td> </tr> </table>	LOW SC-7	MOD SC-7 (1) (2) (3) (4) (5)	HIGH SC-7 (1) (2) (3) (4) (5) (6)								
LOW SC-7	MOD SC-7 (1) (2) (3) (4) (5)	HIGH SC-7 (1) (2) (3) (4) (5) (6)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
SC-8 Transmission Integrity <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-8</td> <td>HIGH SC-8 (1)</td> </tr> </table>	LOW Not Selected	MOD SC-8	HIGH SC-8 (1)								
LOW Not Selected	MOD SC-8	HIGH SC-8 (1)									
SC-9 Transmission Confidentiality <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-9</td> <td>HIGH SC-9 (1)</td> </tr> </table>	LOW Not Selected	MOD SC-9	HIGH SC-9 (1)								
LOW Not Selected	MOD SC-9	HIGH SC-9 (1)									
SC-10 Network Disconnect <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-10</td> <td>HIGH SC-10</td> </tr> </table>	LOW Not Selected	MOD SC-10	HIGH SC-10								
LOW Not Selected	MOD SC-10	HIGH SC-10									
SC-11 Trusted Path <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected								
LOW Not Selected	MOD Not Selected	HIGH Not Selected									
SC-12 Cryptographic Key											

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
Establishment and Management <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-12</td> <td>HIGH SC-12</td> </tr> </table>	LOW Not Selected	MOD SC-12	HIGH SC-12								
LOW Not Selected	MOD SC-12	HIGH SC-12									
SC-13 Use of Cryptography <table border="1"> <tr> <td>LOW SC-13</td> <td>MOD SC-13</td> <td>HIGH SC-13</td> </tr> </table>	LOW SC-13	MOD SC-13	HIGH SC-13								
LOW SC-13	MOD SC-13	HIGH SC-13									
SC-14 Public Access Protections <table border="1"> <tr> <td>LOW SC-14</td> <td>MOD SC-14</td> <td>HIGH SC-14</td> </tr> </table>	LOW SC-14	MOD SC-14	HIGH SC-14								
LOW SC-14	MOD SC-14	HIGH SC-14									
SC-15 Collaborative Computing <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-15</td> <td>HIGH SC-15</td> </tr> </table>	LOW Not Selected	MOD SC-15	HIGH SC-15								
LOW Not Selected	MOD SC-15	HIGH SC-15									
SC-16 Transmission of Security Parameters											

FOR EXAMPLE ONLY

Security Control			L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied		
<table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH Not Selected</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH Not Selected									
LOW Not Selected	MOD Not Selected	HIGH Not Selected										
SC-17 Public Key Infrastructure Certificates												
<table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-17</td> <td>HIGH SC-17</td> </tr> </table>	LOW Not Selected	MOD SC-17	HIGH SC-17									
LOW Not Selected	MOD SC-17	HIGH SC-17										
SC-18 Mobile Code												
<table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-18</td> <td>HIGH SC-18</td> </tr> </table>	LOW Not Selected	MOD SC-18	HIGH SC-18									
LOW Not Selected	MOD SC-18	HIGH SC-18										
SC-19 Voice Over Internet Protocol												
<table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-19</td> <td>HIGH SC-19</td> </tr> </table>	LOW Not Selected	MOD SC-19	HIGH SC-19									
LOW Not Selected	MOD SC-19	HIGH SC-19										
SC-20 Secure Name / Address Resolution Service (Authoritative Service)												

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-20</td> <td>HIGH SC-20</td> </tr> </table>	LOW Not Selected	MOD SC-20	HIGH SC-20								
LOW Not Selected	MOD SC-20	HIGH SC-20									
SC-21 Secure Name / Address Resolution Service (Recursive of Caching Resolver) <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH SC-21</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH SC-21								
LOW Not Selected	MOD Not Selected	HIGH SC-21									
SC-22 Architecture and Provisioning for Name / Address Resolution Service <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-22</td> <td>HIGH SC-22</td> </tr> </table>	LOW Not Selected	MOD SC-22	HIGH SC-22								
LOW Not Selected	MOD SC-22	HIGH SC-22									
SC-23 Session Authority <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SC-23</td> <td>HIGH SC-23</td> </tr> </table>	LOW Not Selected	MOD SC-23	HIGH SC-23								
LOW Not Selected	MOD SC-23	HIGH SC-23									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
Effectiveness Level Reached								

NOTES:

17. System and Information Integrity

Class: Operational

FIPS 199 Impact Level: Low ____ Moderate ____ High ____

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
SI-1 System and Information Integrity Policy and Procedures <table border="1"> <tr> <td>LOW SI-1</td> <td>MOD SI-1</td> <td>HIGH SI-1</td> </tr> </table>	LOW SI-1	MOD SI-1	HIGH SI-1								
LOW SI-1	MOD SI-1	HIGH SI-1									
SI-2 Flaw Remediation <table border="1"> <tr> <td>LOW SI-2</td> <td>MOD SI-2</td> <td>HIGH SI-2(1) (2)</td> </tr> </table>	LOW SI-2	MOD SI-2	HIGH SI-2(1) (2)								
LOW SI-2	MOD SI-2	HIGH SI-2(1) (2)									
SI-3 Malicious Code Protection <table border="1"> <tr> <td>LOW SI-3</td> <td>MOD SI-3 (1) (2)</td> <td>HIGH SI-3 (1) (2)</td> </tr> </table>	LOW SI-3	MOD SI-3 (1) (2)	HIGH SI-3 (1) (2)								
LOW SI-3	MOD SI-3 (1) (2)	HIGH SI-3 (1) (2)									
SI-4 Information System Monitoring Tools and Techniques <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SI-4 (4)</td> <td>HIGH SI-4 (2) (4)</td> </tr> </table>	LOW Not Selected	MOD SI-4 (4)	HIGH SI-4 (2) (4)								
LOW Not Selected	MOD SI-4 (4)	HIGH SI-4 (2) (4)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied			
<table border="1"> <tr> <td></td> <td></td> <td>(5)</td> </tr> </table>			(5)								
		(5)									
SI-5 Security Alerts and Advisories <table border="1"> <tr> <td>LOW SI-5</td> <td>MOD SI-5</td> <td>HIGH SI-5 (1)</td> </tr> </table>	LOW SI-5	MOD SI-5	HIGH SI-5 (1)								
LOW SI-5	MOD SI-5	HIGH SI-5 (1)									
SI-6 Security Functionality Verification <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH SI-6</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH SI-6								
LOW Not Selected	MOD Not Selected	HIGH SI-6									
SI-7 Software and Information Integrity <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD Not Selected</td> <td>HIGH SI-7(1) (2)</td> </tr> </table>	LOW Not Selected	MOD Not Selected	HIGH SI-7(1) (2)								
LOW Not Selected	MOD Not Selected	HIGH SI-7(1) (2)									
SI-8 Spam Protection <table border="1"> <tr> <td>LOW Not Selected</td> <td>MOD SI-8</td> <td>HIGH SI-8 (1)</td> </tr> </table>	LOW Not Selected	MOD SI-8	HIGH SI-8 (1)								
LOW Not Selected	MOD SI-8	HIGH SI-8 (1)									

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied						
SI-9 Information Input Restrictions <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW</td> <td style="text-align: center;">MOD</td> <td style="text-align: center;">HIGH</td> </tr> <tr> <td style="text-align: center;">Not Selected</td> <td style="text-align: center;">SI-9</td> <td style="text-align: center;">SI-9</td> </tr> </table>	LOW	MOD	HIGH	Not Selected	SI-9	SI-9								
LOW	MOD	HIGH												
Not Selected	SI-9	SI-9												
SI-10 Information Accuracy, Completeness, Validity, and Authenticity <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW</td> <td style="text-align: center;">MOD</td> <td style="text-align: center;">HIGH</td> </tr> <tr> <td style="text-align: center;">Not Selected</td> <td style="text-align: center;">SI-10</td> <td style="text-align: center;">SI-10</td> </tr> </table>	LOW	MOD	HIGH	Not Selected	SI-10	SI-10								
LOW	MOD	HIGH												
Not Selected	SI-10	SI-10												
SI-11 Error Handling <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW</td> <td style="text-align: center;">MOD</td> <td style="text-align: center;">HIGH</td> </tr> <tr> <td style="text-align: center;">Not Selected</td> <td style="text-align: center;">SI-11</td> <td style="text-align: center;">SI-11</td> </tr> </table>	LOW	MOD	HIGH	Not Selected	SI-11	SI-11								
LOW	MOD	HIGH												
Not Selected	SI-11	SI-11												
SI-12 Information Output Handling and Retention <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">LOW</td> <td style="text-align: center;">MOD</td> <td style="text-align: center;">HIGH</td> </tr> <tr> <td style="text-align: center;">Not Selected</td> <td style="text-align: center;">SI-12</td> <td style="text-align: center;">SI-12</td> </tr> </table>	LOW	MOD	HIGH	Not Selected	SI-12	SI-12								
LOW	MOD	HIGH												
Not Selected	SI-12	SI-12												

FOR EXAMPLE ONLY

Security Control	L1 Policy	L2 Procedures	L3 Implemented	L4 Tested	L5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
Effectiveness Level Reached								

NOTES:

Appendix G - Miscellaneous Security Templates

Appendix G: Miscellaneous Security Templates

System Disposal Checklist

System Disposal Checklist					
Principal Office:					
System:					
No.	Requirement	Compliance			Comments
		Yes	No	N/A	
1.	All information has been moved to another system, archived, discarded, or destroyed.				
2.	Legal requirements for records retention were considered before disposing of the system.				
3.	All information is cleared and purged from the system.				
4.	All information has been removed from storage medium (e.g., hard disk or tape).				
5.	Appropriate steps have been taken to ensure the level of sanitization is appropriate for the type of storage medium (e.g., overwriting, degaussing (for magnetic media only), and destruction).				
6.	All hardcopy media has been destroyed (e.g., shredded, burned, etc.).				
7.	Appropriate steps have been taken to ensure that all contractors implement sanitization policies and procedures for removing information processed or residing on a contractor's site.				
8.	Leased equipment for processing information has been sanitized before returned to the vendor.				

System Disposal Checklist					
Principal Office:					
System:					
No.	Requirement	Compliance			Comments
		Yes	No	N/A	
9.	When data has been removed from storage media, every precaution has been taken to remove duplicate versions that may exist on the same or other storage media, back-up files, temporary files, hidden files, or extended memory.				

System Owner Printed Name

System Owner Signature

Date

Appendix H - Performance Assessment Sample Questions and Survey

Appendix H: Performance Assessment Sample Questions and Survey

Federal Student Aid/CIO/Quality Assurance

Customer Satisfaction Questionnaire

Contract Reference:

Deliverable or Period:

Scope: Content, Quality & Accuracy of the QA Contractor's involvement

If you feel a question does not apply or you have no opinion please indicate using (NA).
 Exceptional Rating (5) – Provide comments (Highly Recommended).

1. Are you satisfied with the overall quality of work being performed by the QA/IV&V Contractor?
 (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) **RESPONSE:** []

Comments:

2. Do you feel that QA/IV&V task is adding value to your program?
 (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) **RESPONSE:** []

Comments:

3. Was the Contractor Team responsive and flexible to ad hoc meetings, schedule changes, etc.?
 (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) **RESPONSE:** []

Comments:

4. Were the Contractor Team's documents delivered on time or ahead of schedule, free of spelling error or clerical defect, thorough and complete – was the information accurate?
 (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) **RESPONSE:** []

Comments:

5. Did the Contractor activities avoid delays in established schedules and development planning?
 (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) **RESPONSE:** []

Comments:

6. Did Contractor Team personnel interact professionally with Government and Contractor personnel in communicating appropriate information to affected program elements in a timely and cooperative manner?
 (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) **RESPONSE:** []

Comments:

--

Prepared by:**Date:****Title:****Evaluation of Contractor's Performance****Based on Industry Best Practices and IEEE Standards**

Exceptional (5) – Performance meets requirements and exceeds many. The performance of the indicator being assessed was accomplished with no problems, or few minor problems for which corrective actions taken by the Contractor Team were highly effective.

Very good (4) – Performance meets requirements and exceeds some. The performance of the indicator being assessed was accomplished with some minor problems for which corrective actions taken by the Contractor Team were effective.

Satisfactory (3) – Performance meets requirements. The performance of the indicator being assessed was accomplished with some minor problems for which corrective actions taken by the Contractor Team appear satisfactory, or completed corrective actions were satisfactory.

Marginal (2) – Performance does not meet some requirements. The performance of the indicator being assessed reflects a serious problem from which the Contractor Team has not yet identified corrective actions. The Contractor Team's proposed actions appear only marginally effective or were not fully implemented.

Unsatisfactory (1) – Performance does not meet requirements and recovery is not likely in a timely or cost effective manner. The performance of the indicator contains serious problem(s) for which the Contractor Team's corrective actions appear or were ineffective.

Federal Student Aid/CIO/Quality Assurance
Contractor Performance Survey
Reference: Task: Contractor:
Deliverable or Period:
Summarize contractor performance and <i>enter</i> the number that corresponds to the rating for each rating category. (<i>See attached Rating Guidelines</i>) For all ratings of 5 (exceptional), please provide comments.
<p>1. Quality of Product or Service (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) RESPONSE: []</p>
Comments:
<p>2. Cost Control (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) RESPONSE: []</p>
Comments:
<p>3. Timeliness of Performance (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) RESPONSE: []</p>
Comments: Perot Systems always sticks to schedule, no matter what.
<p>4. Business Relations (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) RESPONSE: []</p>
Comments:
<p>5. Is/was the contractor committed to customer satisfaction? (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) RESPONSE: []</p>
Comments:
<p>6. Would you recommend selection of this firm again? (1 ---- 2 ---- 3 ---- 4 ---- 5) (N/A) RESPONSE: []</p>
Comments:

Prepared by:
Title:

Date:

Ratings Guidelines

Summarize contractor performance in each of the rating areas. Assign each area a rating of: 1 (Unsatisfactory), 2 (Fair/Marginal), 3 (Good/Satisfactory), 4 (Excellent/Very good), 5 (Outstanding/Exceptional). Use the following instructions as guidance in making these evaluations. Ensure that this assessment is consistent with any other Agency assessments made (i.e., for payment of fee purposes).

Criteria	Quality of Product or Service	Cost Control	Timeliness of Performance	Business Relations
	<ul style="list-style-type: none"> - Compliance with contract - Accuracy of reports - Effectiveness of personnel - Technical excellence 	<ul style="list-style-type: none"> - Record of forecasting and controlling target costs - Current, accurate and complete billings - Relationship of negotiated costs to actuals - Cost efficiencies 	<ul style="list-style-type: none"> - Met interim milestones - Reliability - Responsive to technical direction - Completed on time including wrap-up and task administration - Met delivery schedules - No liquidated damages 	<ul style="list-style-type: none"> - Effective management including subcontracts - Reasonable/cooperative behavior - Notification of problems - Flexibility - Pro-active vs. reactive - Effective small/small disadvantaged business subcontracting program
1 - Unsatisfactory	Nonconformances are jeopardizing the achievement of task requirements, despite use of Agency resources	Ability to manage cost issues is jeopardizing performance of task despite use of Agency resources	Delays are jeopardizing performance of task requirements, despite use of Agency resources	Response to inquiries, technical/ service/ administrative issues in not effective
2 - Fair/Marginal	Overall compliance requires minor Agency resources to ensure achievement of task requirements	Ability to manage cost issues requires minor Agency resources to ensure achievement of task requirements	Delays require minor Agency resources to ensure achievement of task requirements	Response to inquiries, technical/service/ administrative issues is somewhat effective
3 - Good/Satisfactory	Overall compliance does not impact achievement of task requirements	Management of cost issues does not impact achievement of task requirements	Delays do not impact achievement of task requirements	Response to inquiries, technical/ service/ administrative issues is usually effective
4 - Excellent/ Very good	There are no quality problems	There are no cost management issues	There are no delays	Responses to inquiries, technical/ service/ administrative issues is effective

5 - Outstanding/Exceptional: The contractor has demonstrated an outstanding performance level in any of the above four categories that justifies adding a point to the score. It is expected that this rating will be used in those rare circumstances when contractor performance clearly exceeds the performance levels described as “Excellent.”

Appendix I – IV&V Metrics Dashboard

Appendix I: IV&V Metrics Dashboard

Phase I - CY Q1 FY2005 (Jan05 - Mar05) IV&V Metrics Dashboard

1.1 Task Order Information Award Number: ABCDE123456 Award Date: 1-May-04 Period of Performance: May 2004 - Sept. 2005 Funding Obligated: \$2,603,037.00 Funding Expended: \$1,750,830.30 % Expended: 67% Funding remaining: \$852,206.70 % Remaining: 33%		1.4 IV&V Quarterly Cost Breakdown - CY Q1 FY2005 									
1.2 Quarterly Cost Data IV&V Cost: \$485,267.50 Project Cost: \$10,140,000.00 % IV&V/Project: 2.0%											
1.3 Project-to-Date Cost Data IV&V Cost: \$1,860,940.40 Project Cost: \$41,250,000.00 % IV&V/Project: 4.8%											
2.1 Findings by Lifecycle Phase				2.2 Findings by Severity			2.3 Customer Satisfaction (avg score for qtr)	2.4 Vendor Performance (avg score for qtr)			
Month	Vision	Def.	Const. & Valid.	Imp.	Support	Total	Major	Moderate	Minor	4.4	4.5
Jan-05	0	91	342	0	0	433	80	224	129		
Feb-05	0	29	75	25	0	129	31	70	28		
Mar-05	0	308	274	58	0	640	65	441	134		
Qtrly Total	0	428	691	83	0	1202	176	735	291		
Qtrly %	0%	36%	57%	7%	0%	100%	15%	61%	24%		
3.0 Findings of Interest 1) IV&V stressed the importance of having/implementing a formal SDLC process. Federal Student Aid has responded to this risk and requested a formal SDLC. 2) IV&V has stressed the lack of resolution of security findings from the FISMA reviews, Corrective Action Plans, and Security Risk Assessments. This issue has been added to the Counterpart meetings in order to get these issues resolved. As some of these issues are critical, timely resolution of these issues is also critical to the annual FISMA audit and successful C&A activities. 3) IV&V has noted that operational reviews have not been performed. IV&V has performed two on-site reviews and has found significant findings. 4) The Security Risk Assessment continues to provide findings to Federal Student Aid early in the process to help ensure a successful C&A. Early notification could impact the upcoming FISMA audit.											

Appendix J – Bibliography and References

Appendix J: Bibliography and References

Bibliography and References
Department of Education & Federal Student Aid Guidance Documents
Department of Education, ACS Directive, Handbook OCIO: 1-104, Personal Use of Government Equipment, May 2, 2006
Department of Education, ACS Directive, Handbook OCIO: 1-106, Lifecycle Management (LCM) Directive Framework, December 02, 2005
Department of Education, ACS Directive, Handbook OCIO-01, Handbook for Information Assurance Security Policy, March 31, 2006
Department of Education, ACS Directive, Handbook OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures, March 21, 2006
Department of Education, ACS Directive, Handbook OCIO-07, Handbook for Information Technology Security Risk Assessment Procedures, January 15, 2004
Department of Education, ACS Directive, Handbook OCIO-09, Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures, March 17, 2005
Department of Education, ACS Directive, Handbook OCIO-10, Handbook for Information Technology Security Contingency Planning Procedures, , July 13, 2005
Department of Education, ACS Directive, Handbook OCIO-11, Handbook for Information Technology Security Configuration Management Planning Procedures, July 13, 2005
Department of Education, ACS Directive, Handbook OCIO-13, Handbook for Telecommunications, April 17, 2006
Department of Education, ACS Directive, Handbook OCIO-14, Handbook for Information Security Incident Response and Reporting Procedures, June 26, 2007
Department of Education, ACS Directive, Handbook OIG-1, Handbook for Personnel Security-Suitability Program, January 27, 2003
Department of Education, ACS Directive, Handbook OIG-2, Handbook for Information Security
Department of Education, ACS Directive, Handbook OM:2-104, Occupant Emergency Organizations and Plans, February 7, 2008
Department of Education, ACS Directive, Handbook OM:4-114, Physical Security Program, January 31, 2008
Department of Education, ACS Directive, Handbook OM:5-101, Contractor Employee Personnel Security Screenings, January 31, 2008

Bibliography and References
Department of Education, ACS Directive, Handbook OM:5-102, Continuity of Operations (COOP) Program, August 30, 2007
Department of Education, ACS Directive, Handbook OM-01, Handbook for Classified National Security Information, November 19, 2007
Department of Education, ACS Directive, OCIO: 2-102, Wireless Telecommunications Services
Department of Education, ACS Directive, OCIO: 3-106, Information Technology Security Facility Physical Security Policy
Department of Education, ACS Directive, PMI 368-1, Flexiplace Program, August 30, 1995
Department of Education, Assurance Compliance Guide
Department of Education, Baseline Security Requirements (Draft Version 2.0, undated)
Department of Education, Critical Infrastructure Protection Plan
Department of Education, Federal Student Aid, Enterprise Operational Change Management Plan, Version 1.1, November 7, 2007
Department of Education, Federal Student Aid, Enterprise Testing Standards Handbook, Version 2.0, dated September 17, 2008
Department of Education, Federal Student Aid, General Support System and Major Application Backup Media Handling Policy
Department of Education, Federal Student Aid, Production Readiness Review Process Description, Version 8.0, dated July 25, 2008
Department of Education, Federal Student Aid, Work Products Guide: Version 4.0, September 17, 2007
Department of Education, Information Assurance Communications Guide
Department of Education, Information Assurance Cost Estimation Guide
Department of Education, Information Assurance Program Management Plan (IAPMP)
Department of Education, Information Assurance System Lifecycle Guide
Department of Education, Information Assurance Testing and Evaluation Plan Guide
Department of Education, Information Technology Secure Platform Configuration Guide, August 2004
Department of Education, Information Technology Security Compliance Guide
Department of Education, Information Technology Security Controls Reference Guide

Bibliography and References
Department of Education, Information Technology Security Metrics Program Plan
Department of Education, Information Technology Security Test and Evaluation Guide
Department of Education, Office of Management Facility Services, Property Management Manual, December 2002
Department of Education, Office of the Chief Information Officer, Secure Platform Configuration Guide, dated August 2004 Department of Education, OM: 3-104, Clearance of Personnel for Separation or Transfer
Federal Laws
Clinger Cohen Act of 1996, P.L. 104-106
Computer Fraud and Abuse Act of 1986, Public Law (PL) 99-474
Computer Security Act of 1987, P.L. 100-235
E-Government Act of 2000, P.L. 106-554, Title III – Federal Information Security Management Act (FISMA)
E-Government Act of 2000, P.L. 106-554, Title V – Confidential Information Protection Security and Efficiency Act (CIPSEA) of 2002
Electronic Communications Privacy Act of 1986, PL 99-508
Federal Manager’s Financial Integrity Act of 1986, P.L. 97-255
Freedom of Information Act (FOIA), PL 93-502
Paperwork Reduction Act of 1980, as amended, 35 U.S.C. 44
Privacy Act of 1974 as amended, P.L. 93-579
Privacy Act of 1974, as amended, PL 93-579
Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1988, P.L. 105-220
Federal Regulations and Guidance Documents
“Information Technology Investment Evaluation Guide. Assessing Risks and Returns: A Guide for Evaluating Federal Agencies’ IT Investment Decision-Making.” GAO/AMD-10.1.13 February, 1997
Federal Enterprise Architecture (FEA) Reference Model (http://www.whitehouse.gov/omb/egov/a-2EAModelsNEW2.html)
Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization,

Bibliography and References
and Protection (supersedes Presidential Decision Directive (PDD)-63)
Office of Federal Procurement Policy, Office of Management and Budget, Executive Office of the President. “Best Practices for Using Current and Past Performance Information,” March 2000
U.S. Office of Management and Budget (OMB), “Financial Management Systems,” Circular A-127, July 23, 1993
U.S. Office of Management and Budget (OMB), “Management Accountability and Control,” OMB Circular A-123, December 21, 2004
U.S. Office of Management and Budget (OMB), “Security of Federal Automated Information Resources,” OMB Circular A-130, Appendix III. Washington, DC: OMB
National Institute of Standards & Technology (NIST) Special Publications and Federal Information Processing Standards (FIPS) Publication Documents
FIPS - 132, Guideline for Software Verification and Validation Plans
FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems, February 2004
FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems, March 2006
NIST – 800-18, Revision 1 - Guide for Developing Security Plans for Information Technology Systems, February 2006
NIST 800-115 – DRAFT Technical Guide to Information Security Testing, November 13, 2007
NIST 800-14 -Generally Accepted Best Practices for Securing Information Technology Systems, September 1996
NIST 800-26, Revision 1 - Guide for Information Security Program Assessments and System Reporting Form, August 2005
NIST 800-37, Revision 1 – DRAFT Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach, August 19, 2008
NIST 800-39 – DRAFT Managing Risk from Information Systems: An Organizational Perspective, April 3, 2008
NIST 800-53, Revision 2 - Recommended Security Controls for Federal Information Systems, December 2007
NIST 800-53A – Guide for Assessing the Security Controls in Federal Information Systems, June 2008
NIST 800-60, Revision 1 – Guide for Mapping Types of Information and Information Systems to Security Categories (Vol. 1 & 2), August 2008

Bibliography and References
NIST 800-64, Revision 2 – DRAFT Security Considerations in the System Development Life Cycle, March 14, 2008
NIST 800-80 – DRAFT Guide for Developing Performance Metrics for Information Security, May 4, 2006
NIST 800-88, Revision 1 – Guidelines for Media Sanitization, September 2006
NIST Federal Desktop Core Configuration (FDCC) Listing (http://nvd.nist.gov/fdcc/index.cfm)
NIST Security Configuration Checklist Programs for IT Products (http://csrc.nist.gov/checklists/index.html)
NIST Security Content Automation Protocol (SCAP) (http://nvd.nist.gov/scap.cfm)
External Guidance Documents
“Project Management Handbook for Mission Critical Systems: A Handbook for Government Executives,” Washington, DC 1998
“V&V Research Quarterly” Volume 5, Number 4 October 1998
Carnegie Mellon University, Capability Maturity Model for Software, Version 1.1, Software Engineering Institute, CMU/SEI-93-TR-24, DTIC Number ADA263403, February 1993
Carnegie Mellon University, Key Practices of the Capability Maturity Model, Version 1.1, Software Engineering Institute, CMU/SEI-93-TR-25, DTIC Number ADA263432, February 1993
Carnegie Mellon University, Software Engineering Institute. <i>The Capability Maturity Model: Guidelines for Improving the Software Process</i> , 1995, www.sei.cmu.edu/cmm
Information Systems Audit and Control Association (ISACA). “Standards for Information Systems Control Professionals,” www.isaca.org/standard/iscontrl.htm
Institute of Electrical and Electronics Engineers (IEEE), “Guideline for Software Verification and Validation Plans,” IEEE-Std P1059 and FIPS Publication 132, 1993, http://standards.ieee.org
Institute of Electrical and Electronics Engineers (IEEE), “Standard for Software Verification and Validation,” IEEE-Std-1012, 1998, http://standards.ieee.org
Institute of Electrical and Electronics Engineers (IEEE). “Characteristics of Metrics,” IEEE-Std-12207.1, 1997, http://standards.ieee.org
Institute of Electrical and Electronics Engineers (IEEE). “Glossary of Software Engineering Terminology,” IEEE-Std-610.12, 1990, http://standards.ieee.org
International Organization for Standardization (ISO) 12207, “Software Lifecycle Processes”
International Organization for Standardization (ISO) 9002 “Quality Management Standards and

Bibliography and References

Guidelines”

Titan Systems Corporation, Averstar Group. “A Case Study of IV&V Return on Investment (ROI)”