U.S. Department of Education
Federal Student Aid

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of the AMERICAN MIND™

Production Readiness Review (PRR) Process Description

Version 12.0

Final

July 31, 2012

Document Identifier: FSA_TOQA_PROC_RLS.PRR_001

Document Version Control

Version	Date	Description
12.0	7/31/2012	• Updated logo and presentation template to new FSA branding. • Updated Section 3, PRR Process steps to better reflect current practice. • Added cover slide on PRR Presentation Template to provide guidance on using the template. • Expanded Data Center Readiness slides to provide additional detail on roll-back planning. • Updated Data Center Readiness slides to reflect RTO and RPO tier changes. • Added a slide to address items specifically related to EEBC and PEBC SharePoint releases. • Updated Security Vulnerability Scan slides to provide better tracing of all scan results to resolutions. • Minor updates to Configuration Management slide based on experience from using this slide over the past year. • Updated Lifecycle Documentation slides to reflect LMM Version 1.2. • Updated sign-off pages to reflect personnel changes.
11.0	7/28/2011	• Revised PRR applicability criteria to be based on the operational risk associated with implementing a release (matching the same criteria that are planned by Enterprise Change Management). ECM operational risk determination will determine if PRR applies to a release. • Expanded slide presentation template to incorporate all information from PRR Checklist and include a Sign-off memo at the end of the presentation; removed PRR Checklist and Sign-off memo artifacts from PRR Process (combined three documents into one). • Revised presentation template to include additional information on the business impact of delaying release implementation. • Revised presentation template to include additional information regarding test results with a focus on performance testing. • Revised presentation template to include a slide for reporting status of configuration management audits. • Revised procedures for distributing PRR Meeting Notices and PRR Presentation materials to include the technology office distribution list. • This PRR Process Description document and the associated presentation template completed and passed Section 508 accessibility review by the ED OCIO Assistive Technology Team on 7/26/2011.

Version	Date	Description
10.0	7/30/2010	• Removed sign-off types (i.e. conditional, provisional, etc). • Expanded timeline of events in the PRR process to add planning steps earlier in the project lifecycle and to accommodate an optional review of test data by CIO Enterprise Testing Group. • Minor re-organization of order and titles of information presented in PRR slides. • Re-organized and updated PRR Checklist (Appendix C and D) to improve usability. • Updates to appendices to support changes.
9.0	7/31/2009	• Added LCM Framework reference (Section 1). • Changes to sign-off for large-scale releases (Section 6). • Added System Test Lead, FSA Computer Security Officer, and Responsible ELT Member descriptions to Sign-off requirements (Section 6). • Clarifications to PRR Process steps, including better identification of the role of the QA Team (Section 4). • Reformatted PRR Summary Checklist to portrait layout instead of landscape and removed risk mitigation columns (Appendix C). • Reformatted PRR Summary Checklist Definitions to portrait layout instead of landscape and removed risk mitigation columns (Appendix D). • Updated sample sign-off memo (Appendix E) • Minor editorial changes for grammar, spelling, formatting, etc (entire document).
8.1	01/30/2009	• Modified Applicability section to address concerns related conducting PRRs on infrastructure and toolset changes. • Clarified the sign-off authorities for the CIO signature. • Added Checklist items to cover re-validation of disaster recovery objectives (RTO and RPO) and vulnerability scans. • Minor clarifications in PRR checklist definitions.
8.0	7/30/2008	Major Document Revision includes the following: • Major Checklist updates to reflect stakeholder discussions • New information regarding rationale for holding PRRs • New diagram depicting the role of the PRR in the context of other related activities • Addition of PRR presentation slides • Updated signoff role descriptions • Updates to signature page • Updated terminology based on VDC Configuration Management Database (CMDB) Data Dictionary, ECOM, and Security documents. • Major formatting and editorial changes to conform to the Federal Student Aid Document Template
1.0 - 7.0	6/19/2007	For previous revision history of Versions 1.0-7.0, see Version 7.0

Table of Contents

Document Version Control i

Table of Contents iii

Executive Summary 1

Section 1. Introduction 2

Section 2. Risk-based criteria for conducting a PRR 5

Section 3. PRR Process 7

- **Step 1: LMM Tailoring Plan** 9
- **Step 2: Requirements, Design, Development, and Testing Activities** 9
- **Step 3: Implementation Change Request Created** 10
- **Step 4: Schedule Pre-PRR and PRR** 10
- **Step 5: Reviews by Technology Office Support Areas** 10
- **Step 6: Operational Readiness Review** 11
- **Step 7: Draft PRR Presentation Distributed** 11
- **Step 8: Pre-PRR** 11
- **Step 9: Service Delivery Review (SDR)** 11
- **Step 10: PRR Presentation Distributed** 12
- **Step 11: PRR Presentation and Sign-off** 12
- **Step 12: Release Production Implementation** 13

Section 4. PRR Presentation 14

Section 5. Sign-Off Responsibilities 53

Appendix A - Acronyms and Abbreviations 56

Appendix B - Glossary 60

Executive Summary

The Production Readiness Review (PRR) Process is a quality review of system releases before each release is implemented in Federal Student Aid's (FSA) production environment. The PRR process is intended to keep FSA management informed of critical release activities and is intended to reduce the likelihood of new system releases causing unintended adverse impact to FSA's business or end-users.

The PRR Process also supports the responsibilities of Federal Student Aid's Technology Office, Chief Information Officer (CIO), as described by the Clinger-Cohen Act. These include:

- Developing, maintaining, and facilitating the implementation of sound and integrated information technology architecture.
- Promoting the effective and efficient design and operation of all major information resource management processes.

The PRR serves as the stage gate between the Testing and Implementation Stages (Technical Stage Gate 4), as described in FSA's Lifecycle Management Methodology.

The PRR covers several areas associated with implementing a system release, including: a review of open risks associated with the implementation, testing activities and results for the release, the readiness of the data center to support implementation and operations of the release, security and privacy impacts of the release, configuration management reviews that have taken place, end user support and communication activities that are associated with the release, and the status of documentation needed to support and operate the information system that is being implemented or enhanced by the release. Further, the PRR provides an opportunity for the Integrated Project Team (IPT) to discuss system changes and process improvements with FSA management and relevant stakeholders.

The Enterprise Quality Assurance Program in the Technology Office provides support and oversight for the PRR process while integrated project teams in the different FSA organizational units are responsible for completing the PRR for system releases and infrastructure changes.

Section 1. Introduction

The Production Readiness Review (PRR) Process is a high-level quality assurance review of system releases before the release is implemented in Federal Student Aid's (FSA) production environment. The PRR process is intended to keep FSA management informed of critical release activities and is intended to reduce the likelihood of new system releases causing unintended adverse impact to FSA's business or end-users. PRR confirms to FSA Management that appropriate system and software development lifecycle activities have occurred in support of the release.

1.1 Purpose

The Production Readiness Review (PRR) Process Description defines Federal Student Aid's approach for conducting PRR activities prior to implementing a system release. This process description provides guidance to individuals responsible for, or involved in these efforts.

1.1.1 Scope

This document defines FSA's PRR process that is used by system development and support teams. The PRR is conducted prior to the implementation of a release of an information system to FSA's production environment, regardless of data center location of the information system. The PRR Process applies to all organizational units and systems within the Federal Student Aide Enterprise. The PRR Process provides for standardized documentation and communication of quality review information.

1.2 Intended Audience

Table 1-1 lists the individuals this document applies to and the purpose for which they may utilize the information in this document.

Intended Audience	Uses
FSA Management	Provides guidance on participation and sign-off responsibilities in the PRR Process.
FSA systems development, operations, maintenance, and infrastructure staff	Provides guidance on information gathering, preparation, presentation, participation and sign-off responsibilities in the PRR Process.
System Support Contractors	Provides guidance on the PRR Process in order to appropriately support FSA as the review activities occur for each system release.

Table 1-1: Intended Audience and Uses

1.3 Document Organization

This document comprises the following sections:

- Section 1 – Introduction: describes the reason and background for this document.
- Section 2 – Risk-based criteria for conducting a PRR
- Section 3 – PRR Process
- Section 4 - PRR Presentation
- Section 5 – PRR Sign-off Responsibilities
- Appendix A – Acronyms and Abbreviations: provides a list of acronyms and abbreviations
- Appendix B – Glossary: defines terminology within the context of this process

1.4 References and Related Documents

This following references and related documents support and impact the PRR Process Description:

- Clinger-Cohen Act of 1996 (Public Law 104-106)
- Privacy Act of 1974 (Public Law 93-579)
- E-Government Act of 2002 (Public Law 107-347)
- Government Performance and Results Act of 1993 (Public Law 103-62)
- Lifecycle Management (LCM) Framework, ED OCIO, July 16, 2010
- Lifecycle Management Methodology (LMM), Federal Student Aid, Version 1.2, June 15, 2012.
- LMM Stage Gate Process Description, Federal Student Aid, Version 1.2, June 15, 2012.
- Enterprise Change Management Plan, Draft Version 1.0, Federal Student Aid, April 20, 2011
- Procuring Electronic and Information Technology (EIT) in Conformance with Section 508 of the Rehabilitation Act of 1973, ED OCIO, ACS Directive OCIO:3-105, September 28, 2010
- Information Technology Investment Management (ITIM) and Software Acquisition Policy, ED OCIO, ACS Directive OCIO:3-108, March 4, 2010
- Enterprise Test Management Standards, Version 3.0, Federal Student Aid, November 8, 2010.
- Circular A-130 – *Management of Federal Information Resources*, OMB, November 28, 2000.
- Federal Information Processing Standards (FIPS) 199 – *Standards for Security Categorization of Federal Information and Information Systems*, NIST, February 2004.

- Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* NIST, August 2008.
- Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* NIST, February 2010.
- Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* NIST, August 2009

Section 2. Risk-based criteria for conducting a PRR

A Production Readiness Review (PRR) is required for application system releases or infrastructure changes that have a high operational risk associated with implementation. System releases and infrastructure changes that have a medium operational risk will hold a PRR at the discretion of the Enterprise Change Control Board (ECCB) based on an informed analysis of the specific risk characteristics of the release. System releases and infrastructure changes with a low operational risk are not required to perform a PRR, but have the option of performing a PRR at the discretion of the Project Manager or Project Sponsor.

The risk ratings are high, medium, and low and are based on the following seven categories:

- System Criticality – system is categorized as critical, important, or supportive.
- System End User Type and Volume – external or internal to FSA and the volume/audience impacted
- Complexity – the scope and intricacies of the change (simple, multifaceted, intricate).
- Size – the change in configuration items or functionality to the system or system components (major, minor, patch – see definitions in the glossary under System Release Type)
- Technology – new to the market or FSA's operating environment, or out-of-support
- Maturity – system's age or support organization's time in supporting system
- Business Cycle – Proposed time for the change to be implemented based on the system's use and processing schedule and potential peak processing of other systems.

The table below is used to determine the operational risk associated with a system release or infrastructure change. The "high water mark" method is used when determining the risk rating. A single risk category being rated higher moves the overall evaluation into the higher rating.

Category	High	Medium	Low
System Criticality	Critical or important	Critical, important, or supportive	Important or supportive
System End User Type and Volume	External – Public / Students / Schools Internal – organization-wide audience of ED / FSA Employees or contractors	External – Title IV Partners Internal – Significant audience of ED / FSA Employees or contractors	Internal – Limited audience of ED / FSA employees, contractors, or auditors
Complexity	Intricate	Multifaceted	Simple
Size	Major or minor	Minor or patch	Patch
Technology	New to FSA, new to market, or out-of-support	Currently supported in FSA environment, but not the exact version/ model	Exact version/ model used is currently supported in FSA environment

Category	High	Medium	Low
Maturity	Federal project management team is new to FSA or releases of this scope. OR Development team (contractor) is new to FSA.	Federal project management team has performed similar releases. OR Development team (contractor) has completed similar projects at FSA.	Federal project management team has performed previous releases of this system. AND Development team (contractor) has preformed previous releases of this system.
Business Cycle	During peak processing period for the system or another impacted system's peak processing period	Prior to peak processing period, but inadequate time to complete first live batch and make corrections	During low point(s) in the processing cycle(s)

Table 2-1: Operational Risk Ratings

The Enterprise Change Control Board (ECCB) has responsibility for assigning operational risk, which determines the requirement for a PRR. The Technology Office, Enterprise Quality Assurance Team will make an initial assessment of Operational Risk which is then reviewed by the ECCB for a final determination. ECCB determinations of Operational Risk for each release and infrastructure change are documented in the bi-weekly Enterprise Master Release Schedule.

A PRR is not required for an emergency change to the production environment (see "change priorities" in Appendix B – Glossary for definition of an emergency change).

Section 3. PRR Process

The following table provides the process steps and timeline for the PRR Process. The Integrated Project Team (IPT) developing a system release or infrastructure change has responsibility for carrying out the steps below with support from many other teams throughout the organization. It is understood that the exact timing of releases and infrastructure changes will be driven by project dependencies and other constraints such as legislative and operational requirements. The steps in the table are explained in detail following the table.

#	PRR Process Step	Timeframe (T = Production Date)	Responsible Group
1	LMM Tailoring Plan completed and LMM Artifacts and Processes incorporated in project schedule.	Project inception and monitored throughout project.	IPT: Sr. Project Manager IT Project Manager Business Project Manager System Technical Lead COTR, ISSO, Test Lead, etc.
2	IPT carries out requirements, design, development, and testing activities consistent with LMM and applicable system/software development methodologies. Note: Regular project updates should be provided to the Technology Office, Quality Assurance Team so that this group is in touch with the project throughout the lifecycle. This can be accomplished by including the QA Team in regularly scheduled status meetings, copying the QA Team on regular status reports, etc.	Based on project schedule.	IPT - Leads Technology Office, QA Team – Participates / stays informed
3	Implementation change request created Note: For VDC hosted systems, this is done through the VDC CCM Tool in the FSA Rational Environment.	Based on project schedule. 3 – 6 months before release implementation date. Prefer that this ticket is opened as soon as project has a realistic implementation date and that change request ticket is updated if implementation dates change.	IPT and/or Application Support Contractor
4	Schedule Pre-PRR and PRR	Minimum of 3 weeks before the Pre-PRR and PRR events. Prefer that this scheduling is done as soon as project has realistic dates for Pre-PRR and PRR Activities.	IPT

#	PRR Process Step	Timeframe (T = Production Date)	Responsible Group
5	Reviews by Technology Office support areas and ISSO: - Enterprise Testing Team (ETT) Reviews Test Results for all phases of testing (System, Performance, 508, UAT, etc.) for projects where manages/supports test efforts. - System Owner and ISSO Security Review - Security Vulnerability Scans conducted - Configuration Management Audits (Functional Configuration Audit and Physical Configuration Audit)	Based on project schedule. Started before Pre-PRR, must complete before PRR.	IPT Technology Office Support Areas
6	Operational Readiness Review (ORR)	Based on project schedule. Must occur before Pre-PRR.	IPT
7	Draft of PRR Presentation distributed	T – 15 business days Must occur before Pre-PRR.	IPT
8	Pre-PRR	T – 14 business days	IPT Technology Office
9	Service Delivery Review (SDR) by Data Center Contractor. A review of the Configuration Management Database entries for the system is performed as part of the SDR. Note: This step may not be required or may be addressed differently if the system is not hosted at the VDC.	If applicable, SDR must be completed prior to PRR. Any outstanding issues from SDR must be reported at PRR.	IPT Virtual Data Center
10	PRR Presentation distributed	T – 8 business days	IPT
11	PRR Presentation and Sign-Off	T – 5 business days	IPT Technology Office
12	Release Production Implementation	T	IPT Technology Office Support Contractors – Application, Middleware, and Data Center

Table 3-1: PRR Process Steps

Step 1: LMM Tailoring Plan

Step 1 of the PRR Process occurs during the initial planning of a system release or infrastructure change project, when the IPT completes the LMM Tailoring Plan (see Lifecycle Management Methodology document for additional information on completing the LMM Tailoring Plan). The LMM Tailoring Plan is developed to support the size, scope, and complexity of the particular project, system, release, or infrastructure change. The lifecycle documentation that applies to the project is identified in the LMM Tailoring Plan and each document should be identified in the project schedule. The LMM also includes several processes, such as Requirements Management, Configuration Management, and Test Management, that should be incorporated into project planning and schedules.

In addition to the lifecycle documents identified in the LMM Tailoring Plan, the following key activities should also be identified in the project schedule:

- Stage Gate Review activities (identified by the LMM)
- Requirements elicitation and documentation or requirements update activities
- Design or design update activities
- System Development activities
- Testing activities, to include applicable test phases (System, Performance, 508, User Acceptance, etc.)
- SORN Publication or updates, if needed.
- OMB Information Collection Clearance approval, if needed.
- Security posture review activities by ISSO (identified as a separate item, but may be grouped with design or in other sections)
- Security Vulnerability Scanning activities
- Configuration Management Activities (schedule activities identify when baselines will be created and when CM audits will be performed)
- Operational Readiness Review (ORR) activities performed internally by the project team
- Service Delivery Review (SDR) activities, if applicable
- Pre-PRR and PRR activities

The list of activities described in this step is not an exhaustive list to build a project schedule, but indicates common areas of concern for PRR participants.

Step 2: Requirements, Design, Development, and Testing Activities

During Step 2 of the PRR Process, the IPT carries out the requirements, design, development, and testing work associated with delivering a system release or infrastructure change. While these activities are ongoing, the Technology Office Quality Assurance Team and other support areas stay informed of project activities and provide guidance and support when needed. The preferred method for this involvement is attendance at regular project status meetings and inclusion on regular project reporting. Meeting notices and other information for this step should be sent to the Quality Assurance Team distribution, “FSA Enterprise Quality Assurance” in the Outlook Global Address List.

Step 3: Implementation Change Request Created

Once the IPT has determined a production implementation date, a change request should be opened with the data center to schedule the production implementation. For the VDC, this is done in the VDC CCM Tool (Rational ClearQuest). This change request is used by several support areas in the Technology Office to monitor the planned implementation date of system releases and infrastructure changes. VDC Change Requests should be opened as far in advance of the release as possible to allow appropriate planning of resources to support the release.

Operational Risk and official determination if a PRR is needed for a particular release will be addressed by the Enterprise Change Control Board (ECCB) based on opening the implementation change request. Therefore, it is critical that this change request be opened as early in the life of a release or infrastructure change as possible.

Step 4: Schedule Pre-PRR and PRR

The Pre-PRR and PRR meetings should be scheduled once the IPT is confident that their development schedule is realistic and finalized. The Pre-PRR takes place a minimum of 14 business days before the production implementation date and the PRR takes place a minimum of five business days before the production implementation date. Meeting notices (Outlook Appointments) for the Pre-PRR and PRR should be sent to the distribution list "Production Readiness Review – Technology Office" and to all members of the IPT.

Step 5: Reviews by Technology Office Support Areas

In preparation for the Pre-PRR and PRR, the IPT and representatives from several different areas of the Technology Office perform reviews of critical deliverables and activities to make sure that the release is ready for production. These reviews include:

- Review of test documentation and results - The Technology Office Enterprise Testing Team reviews the test documentation for the release and the results of test execution. This includes all applicable test phases (System, Performance, 508, User Acceptance, etc.). The Enterprise Test Team performs this review for releases where that team manages/supports the testing effort, not for every release.
- The Technology Office Enterprise Performance Test (EPT) Team evaluates each release to determine if performance testing is appropriate. If performance testing is recommended, the team conducts the testing and works with the IPT to address any defects. The EPT Team reports on final performance test results at the PRR.
- Security posture review – the ISSO and System Owner for review how the changes being implemented in the release impact the security controls of the system. The ISSO and System Owner review the changes that are being implemented with the release; in particular those changes affecting system architecture and application design, and determine if those changes alter the security controls of the system (defined in the system security plan). If those controls are changed, by the release or gain/lose effectiveness as a result of the release, then the security posture of the system is impacted and this impact should be described as part of the PRR. In addition, the ISSO ensures that security documentation for the system has been updated to reflect the changes in the release. The

security posture review is a substantial review effort that will require participation by the entire IPT.

- Security Vulnerability Scanning – the ISSO coordinates vulnerability scanning and analysis, supported by the Technology Office Cyber Security Team.
- Configuration Management – Prior to the PRR, all Configuration Management audits of the software product (functional configuration audit and physical configuration audit) should be completed and the final product baseline should be completed.
- Quality Assurance – Prior to the PRR, the Technology Office Enterprise Quality Assurance Team may review certain system, release, or project-specific documentation. The selection of this documentation will vary based on the particular release. This review will be high-level to make sure that documentation is in place and makes sense in the context of the release. For example, if Quality Assurance selects the System Security Plan for review, the plan will be reviewed at a high level with a sampling of security controls reviewed, not a verification of every security control. A request to perform a QA review prior to the PRR will be communicated to the project manager and/or the system technical lead.

Step 6: Operational Readiness Review

Step 6 of the PRR Process is for the IPT to hold an internal Operational Readiness Review. The content and level of formality of this review is completely at the discretion of the IPT. The outcome of this review should be to determine if the release or infrastructure change is ready to be presented at the Pre-PRR and PRR.

Step 7: Draft PRR Presentation Distributed

Step 7 of the PRR Process is for the IPT to create the PRR Presentation using the PRR Presentation Template and to distribute the presentation to the distribution list “Production Readiness Review – Technology Office” and to all members of the IPT.

Step 8: Pre-PRR

The Pre-PRR is a rehearsal of the Production Readiness Review meeting and an opportunity for the reviewers of the Draft PRR Presentation (step 7) to ask questions about the content of the presentation. The Pre-PRR should be scheduled for 14 business days before the implementation of the release or infrastructure change in the production environment. Participants in the Pre-PRR should ask any questions that they have in this forum and in particular any questions that will require additional research or follow-up by the IPT. The participants in the Pre-PRR should identify any changes needed to complete the PRR Presentation. The determination for second-level sign-off by FSA Senior Management should be discussed at the Pre-PRR to make sure that all parties are aware of the need to brief their Operating Committee members. The IPT should follow up on any outstanding questions before the PRR meeting.

Step 9: Service Delivery Review (SDR)

The Service Delivery Review (SDR) is a review performed by the data center provider (this review may have a different name for data centers other than the VDC). SDR reviews the

information that the data center needs to provide support to the system. The SDR process is the responsibility of the data center provider. For additional information on SDR, contact the FSA VDC Manager.

In addition, the Configuration Management Database (CMDB) entries are reviewed as part of the SDR. In preparation for the SDR, the System Technical Lead should request a copy of the system's current CMDB report from the Technology Office Configuration Management Team, using the FSA Enterprise CMDB Requests mailbox in MS Outlook. This CMDB report should be reviewed by the System Technical Lead and any updates should be sent to the FSA Enterprise CMDB Requests mailbox. This review and update process often takes several days and should be coordinated well in advance of SDR and PRR.

If it is determined that an SDR is not needed for a particular release, the System Technical Lead still completes CMDB review and update described in this step.

Step 10: PRR Presentation Distributed

The final version of the PRR Presentation, including all changes identified in the Pre-PRR, should be distributed three business days before the PRR. For this final distribution, the PRR Presentation should be complete. There is some schedule flexibility to ensure that complete and accurate information is included in the PRR Presentation, but the published standard is that the presentation should be distributed three business days prior to the PRR. Please contact the Enterprise Quality Assurance Team if a team needs flexibility to distribute a PRR Presentation less than three business days before the PRR.

Step 11: PRR Presentation and Sign-off

The PRR Meeting is scheduled for five business days before the implementation of a system release or infrastructure change. Participants in the PRR meeting include the IPT and all the individuals listed as required signatories in Section 6 (or their designees). In addition, support staff also attend the meeting to answer specific questions and provide clarifications. The PRR Presentation should last approximately one hour and should be delivered by Federal staff (contractors should not lead the meeting), such as the Project Manager, Technical Lead, or another member of the IPT that is assigned this responsibility. It is recommended that different members of the IPT brief sections of the presentation associated with their responsibilities (i.e. the test lead briefs the testing slides, the ISSO briefs the security slides, etc.).

At the conclusion of the meeting, the final slides of the PRR Presentation should be signed, indicating that the system release or infrastructure change is formally authorized to be implemented in the production environment.

In some cases, PRR signatories will request that the PRR slides be updated and redistributed with information and clarifications that was discussed during the meeting. In those cases, the Project Manager or System Technical Lead is responsible for making the updates and distributing the final set of slides.

Step 12: Release Production Implementation

The PRR is the final formal activity for FSA Management regarding the implementation of a production release. Once the release has been authorized, the data center and/or application team implementing the release follow an hour-by-hour plan to implement the release. As part of this hour-by-hour plan, a go or no-go decision is made by the technical team to ensure that the application or infrastructure change is working as expected.

If a no-go decision is made, the team follows a back-out plan to remove the release or change from production and restore normal operations. The release would then be rescheduled for implementation after changes and fixes have been made to the release package. When a release is backed-out, a new PRR may be required by the ECCB; however, the normal procedure is that a new PRR is not required.

After the release is implemented, the System Technical Lead should repeat the CMDB request and update described in Step 9. Another copy of the CMDB report is reviewed to ensure that changes have been applied to the CMDB and that the version numbers are correct for items that were implemented in production (after implementation, the CMDB versions should match production).

Section 4. PRR Presentation

The PRR Presentation described in this section may be customized to meet the needs of the specific system release or infrastructure change undergoing review; however, all information included in the PRR Presentation Template must be covered during the presentation. The standard agenda items that must be covered by the PRR Presentation include:

1. Business Background of System
2. Scope of this release
3. Schedule Overview
4. Review of Open Risks
5. Testing Activities and Results
6. Data Center Readiness
7. Security & Privacy
8. Configuration Management
9. Documentation needed for Implementation and Operations
10. End User Support and Communication
11. Lessons Learned
12. Meeting Closure and Sign-off

Additional information and issues may be added to the PRR presentation, as necessary. If an item listed in the presentation template does not apply, the IPT should indicate that it does not apply and explain why it does not apply to the release.

The following slides from the PRR Presentation Template describe the information to be presented during the PRR. Additional guidance is provided in this document (under each slide image) for completing each of the slides. A PowerPoint version of this template is available to assist in creating the PRR Presentation. Please access the LMM site on EEBC/SharePoint using the following link for the PowerPoint version of the PRR Template as well as other LMM documents.

Link to LMM Site on EEBC/SharePoint: LMM SharePoint Library

Production Readiness Review

Presentation Template

Version 12.0
FINAL
July 31, 2012
Document Identifier: FSA_TOQA_STDS_RLS.PRR_001

Template Instructions:
The following slides are provided as a guide to developing PRR presentations.

- It is expected that the slides will be adjusted to fit the needs of particular releases; information requested by this template should be included in the presentation in a way that is understandable within the context of the release.
- Information in [blue and brackets] is guidance and should be deleted and replaced with release-specific information. PRR Presentations should not include [brackets]. Black text, outside of brackets, should be left as part of the presentation.
- Please remove this cover slide when using the template to create a PRR Presentation.
- Detailed slide-by-slide guidance is included in the PRR Process Description Document, please refer to that document when preparing for a PRR.

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 1:
Slide 1 is the cover page for the PRR Template. This slide provides high-level guidance on the template and points the user of the template to this process description document. This slide should be deleted from the presentation as the first step in preparing the Draft PRR Presentation.

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of the AMERICAN MIND™

[System Name and Release Number]

Production Readiness Review

[Date]

[Document Identifier – Technology Office PRRs, please contact CM Team for a Document Identifier. All others, please delete the document identifier item.]

Guidance for Slide 2:

Slide 2 is the cover page for the PRR Presentation. This slide should include the system name, the system component name (if applicable), the release number (for application changes), and the date of the PRR Presentation. PRR presentation documents (along with other project documents) generated by the Technology Office should include a document identifier which will be provided by the Configuration Management Team upon request. Note that once you have removed slide 1, this slide will be the first slide in the presentation and all other slides in the template will re-number.

Agenda

1. Business Background of System
2. Scope of this release
3. Schedule Overview
4. Review of Open Risks
5. Testing Activities and Results
6. Data Center Readiness
7. Security & Privacy
8. Configuration Management
9. Documentation needed for Implementation and Operations
10. End User Support and Communication
11. Lessons Learned
12. Meeting Closure and Sign-off

3

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 3:
Slide 3 is the agenda for the PRR Presentation. This slide should include the twelve standard agenda items listed in the template and any additional items that the IPT would like to cover.

[System] Business Background

[Describe the business purpose of the system in general.

Describe legislative requirements that the system supports.

Describe major FSA functions that are performed by the system.

Describe technology used by the system at a high level. This includes development tools, software languages, database system used, and major components that are being leveraged.

Example:

ABC was developed in Drupal and uses MySQL Enterprise database.

ABC utilizes the General Service Administration USASearch engine.

Describe number and type of users supported by the system]

4

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 4:

This slide should describe the business mission of the system, business functions of the system, the major technologies used, and the users supported. This slide is intended to provide management with an overview of the main functions of the system. This slide should be written at a level so that a manager who is unfamiliar with the system can learn about the purpose of the system.

Scope of Release [Insert Release #]

[Describe the scope of the release that is being implemented.

Describe the business benefits that will be realized by implementing this release.

Describe the technology changes being implemented by this release.

Examples: new functionality to meet a legislative requirement, improvements to the user experience, moves the system to a more current version of a product, expands capacity, etc.]

The build number of this release is: [obtain number from system's configuration manager]

5

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slides 5-6:
Slides 5 and 6 describe the scope of the specific release. These slides should address the changes that are being made to the system, what legislation is impacting the changes, and the benefits/expected improvements that will result from implementation of the release or infrastructure change.

There should be a statement addressing the business impact of delaying implementation of the release. This provides context to PRR participants throughout the rest of the presentation, so that it is understood if there is a legislative deadline or other business driver that would conflict with possible corrective actions.

In addition, for any release that includes a software build, the specific build number of the software being implemented in production should be included to describe the scope of the release – this information may be obtained from the system's configuration manager.

Scope of Release [Insert Release #]

[Describe the business impact of delaying implementation. Include the maximum implementation delay that could be tolerated and still meet FSA's business objectives.

If there is a legislative or regulatory deadline associated with this implementation, please include that information.]

6

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slides 5-6:
Slides 5 and 6 describe the scope of the specific release. These slides should address the changes that are being made to the system, what legislation is impacting the changes, and the benefits/expected improvements that will result from implementation of the release or infrastructure change.

There should be a statement addressing the business impact of delaying implementation of the release. This provides context to PRR participants throughout the rest of the presentation, so that it is understood if there is a legislative deadline or other business driver that would conflict with possible corrective actions.

In addition, for any release that includes a software build, the specific build number of the software being implemented in production should be included to describe the scope of the release – this information may be obtained from the system's configuration manager.

Schedule Overview

	Planned (baseline) Completion	Actual Completion
Requirements	1/30/2008	2/30/2008
Requirements Review (LMM Technical Stage Gate 3)	2/3/2008	3/3/2008
Design	2/30/2008	4/20/2008
Design Review (LMM Technical Stage Gates 1A and 1B)	3/5/2008	5/5/2008
Development	5/30/2008	7/30/2008
Test Readiness Review for System Test (LMM Technical Stage Gate 2)	6/1/2008 – 6/5/2008	8/1/2008 – 8/5/2008
System Testing	6/15/2008	8/15/2008
Intersystem Testing	6/30/2008	8/30/2008
508 Compliance Testing	6/30/2008	8/15/2008
Performance Testing	8/10/2008	10/10/2008
Test Readiness Review for User Acceptance Testing (LMM Technical Stage Gate 2)	7/5/2008 – 7/10/2008	8/20/2008 – 8/30/2008
User Acceptance Testing	7/30/2008	9/30/2008
Code Freeze (start and end)	8/1/2008 – 8/14/2008	10/1/2008 - 10/31/2008
Security Vulnerability Scanning	8/14/2008	10/14/2008
SDR	8/15/2008	10/15/2008
PRR (LMM Technical Stage Gate 4)	8/30/2008	10/30/2008
Production Cutover	9/1/2008	11/1/2008

7

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 7:

Slide 7 covers a high-level view of the project schedule for the release or infrastructure change. The items included in the template generally apply to an application release. The IPT may tailor this slide, however removal of items will likely result in questions from PRR participants, so an explanation of removed activities may be needed. It is understood that PRRs for infrastructure changes may need to significantly tailor the schedule slide to align with infrastructure activities. Actual completion dates listed on this slide should reflect the actual date that an activity was completed and not closure dates from tracking tickets that may lag an actual date by several days.

Review of Open Risks

Risk Name	Risk Description	Probability	Impact	Mitigation Strategy	Risk Owner
		[High]	[High]		
		[Moderate]	[Moderate]		
		[Low]	[Low]		

[Note: This slide should include only the risks related to deploying this release to production, not the entire project risk register.]

Probability	
Scale	Definition
High	Risk has a 50% or greater chance of occurring. Risk is more likely to occur than not.
Moderate	Risk has a greater than 10% and less than 50% chance of occurring
Low	Risk has a 10% or less chance of occurring

Impact	
Scale	Definition
High	If realized, the risk results in an inability to meet business mission/outcomes of the system.
Moderate	If realized, the risk results in a degraded ability to meet business mission/outcomes of the system.
Low	If realized, the risk results in annoyance or inconvenience, but the business mission/outcomes of the system will continue to be met.

8

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 8:

Slide 8 provides the PRR Participants with a listing of the open risks related to implementing a release or infrastructure change in the production environment. This slide should only cover risks specific to the implementation and immediate production operations of the system. It should not include project risks outside of those that specifically relate to the production implementation. The scale at the bottom of the slide for evaluating probability and impact should be used to provide context to each risk identified. The risk of a management decision not to implement the release (i.e. a no-go at the PRR) should not be included – that information is covered on slide 6, as part of the business impact of delaying implementation of the release.

Testing Activities

Test Phase	Organization Executing Tests	Status of Testing
System Testing – System Testing evaluates the integrated system (application) as a whole. The Testing Team performs tests to ensure that each function of the system works as expected and that any errors are documented, analyzed, and resolved appropriately.	[Company Name of Contractor / Federal Student Aid Team]	[Not Performed / In Progress / Complete – For responses of Not Performed or In Progress, please provide explanation.]
Intersystem Testing – Testing of the interfaces between systems.	[Company Name of Contractor / Federal Student Aid Team]	[Not Performed / In Progress / Complete – For responses of Not Performed or In Progress, please provide explanation.]
Accessibility (508) Testing – Testing to ensure that employees and members of the public with disabilities have access to and use of information that is comparable to that available to individuals without disabilities.	ED OCIO Assistive Technology Team	[Not Performed / In Progress / Complete – For responses of Not Performed or In Progress, please provide explanation.] [Only the ED OCIO Assistive Technology Team can determine that 508 testing is not needed for a release. If this determination is made, please include an e-mail from that team confirming the decision.]
Performance testing – Test the performance characteristics of the system, including user load and throughput for the user interface, transaction/batch processing, and database.	FSA Enterprise Performance Test (EPT) Team	[Not Performed / In Progress / Complete – For responses of Not Performed or In Progress, please provide explanation.]
User Acceptance Testing – Formal testing with respect to Application Owner needs, requirements, and processes conducted to determine whether a system satisfies the acceptance criteria and to enable the user, customers, or other authorized entity to determine whether to accept the system.	Federal Student Aid [FSA Office Name]	[Not Performed / In Progress / Complete – For responses of Not Performed or In Progress, please provide explanation.]

9

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 9:

Slide 9 gives an overview of the testing activities that were performed. The template includes rows for system testing, intersystem testing, accessibility (508) testing, performance testing, and user acceptance testing. If additional phases of testing were done for a particular release or infrastructure change, then a row should be added for each additional test phase. The five test phases (rows) listed in the template should not be deleted – if one of the test phases does not apply, it should be marked as "Not Performed" and an explanation provided under the "Status of Testing" column. The text in the "Test Phase" column should not be changed, except to add and describe an additional phase of testing. The "Organization Executing Test" column should be updated to reflect the organization that did the actual test execution (for contractors, the Prime Contractor should be listed, sub-contractors should not be listed).

Test Results Summary

Type of Testing	# Test Cases/ Scripts	DEFECTS OPENED					DEFECTS CLOSED					DEFECTS DEFERRED					DEFECTS RESULTING IN ENHANCEMENTS				
		Urgent	High	Med	Low	Total	Urgent	High	Med	Low	Total	Urgent	High	Med	Low	Total	Urgent	High	Med	Low	Total
System	50	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
Intersystem	30	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
Accessibility	20	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
Performance	10	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
User Acceptance	100	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
TOTALS	210	20	20	20	20	80	5	5	5	5	20	5	5	5	5	20	10	10	10	10	40

Defect Severity Levels

Urgent – Prevents the accomplishment of an operational or mission essential capability

High – Adversely affects the accomplishment of an operational or mission essential capability and no work around solution is known.

Medium – Adversely affects the accomplishment of an operational or mission essential capability, but a work around solution is known and productivity is negatively impacted.

Low – Results in user inconvenience or annoyance but does not affect a required operational or mission essential capability.

10

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 10:

Slide 10 includes a table that shows the basic defect counts from testing. These include the number of test cases/scripts executed, the number of defects opened, the number of defects closed, the number of defects deferred, and the number of defects that resulted in system enhancement requests for each phase of testing. The defects are categorized by severity into urgent, high, medium, and low. The definitions of severity provided in the slide template match Federal Student Aid's Enterprise Test Management Standards. If the IPT wants to use different categories or severity levels, please consult with the Technology Office Enterprise Testing Team to tailor this slide.

System Test Results

Open Defects: [note: FSA generally does not implement releases with open urgent or high defects]

- Medium: [provide description of the defect and the business functionality impacted by the defect]
- Low: [provide description of the defect and the business functionality impacted by the defect]

Closed Defects: [note: only provide urgent and high for closed defects]

- Urgent: [provide description of the defect and the business functionality impacted by the defect]
- High: [provide description of the defect and the business functionality impacted by the defect]

11

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 11:

Slide 11 includes a description of open defects as well as the closed urgent and high severity defects that were encountered during system testing. All open defects should be explained on this slide. Urgent and High defects that were encountered during testing should also be explained briefly (even when those defects are closed). If there are a large number of defects, statuses may be summarized to cover the types of errors found. Descriptions must be provided in full for urgent defects. Defect reports may be provided as an appendix to the PRR rather than listing large numbers of defects in the slides. In general, releases will not be approved at the PRR with urgent or high severity defects that are still open. If an exception to this is needed, please consult with the Enterprise Testing Team prior to the PRR to review the particular situation.

Intersystem Test Results

Open Defects: [note: FSA generally does not implement releases with open urgent or high defects]

- Medium: [provide description of the defect and the business functionality impacted by the defect]
- Low: [provide description of the defect and the business functionality impacted by the defect]

Closed Defects: [note: only provide urgent and high for closed defects]

- Urgent: [provide description of the defect and the business functionality impacted by the defect]
- High: [provide description of the defect and the business functionality impacted by the defect]

12

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 12:
Slide 12 includes a description of open defects as well as the closed urgent and high severity defects that were encountered during intersystem testing. All open defects should be explained on this slide. Urgent and High defects that were encountered during testing should also be explained briefly. In general, releases will not be approved at the PRR with urgent or high severity defects that are still open. If an exception to this is needed, please consult with the Enterprise Testing Team prior to the PRR to review the particular situation.

Accessibility Test Results

Open Defects: [note: FSA generally does not implement releases with open urgent or high defects]

- Medium: [provide description of the defect and the business functionality impacted by the defect]
- Low: [provide description of the defect and the business functionality impacted by the defect]

Closed Defects: [note: only provide urgent and high for closed defects]

- Urgent: [provide description of the defect and the business functionality impacted by the defect]
- High: [provide description of the defect and the business functionality impacted by the defect]

13

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 13:
Slide 13 includes a description of open defects as well as the closed urgent and high severity defects that were encountered during accessibility (508 compliance) testing. All open defects should be explained on this slide. Urgent and High defects that were encountered during testing should also be explained briefly. In general, releases will not be approved at the PRR with urgent or high severity defects that are still open. If an exception to this is needed, please consult with the Enterprise Testing Team prior to the PRR to review the particular situation.

Note: The test report provided by the ED OCIO Assistive Technology Team (the group responsible for accessibility testing) does not categorize defects by severity. The Test Lead should categorize the defects from this report.

Performance Test Results

[Please contact the Enterprise Performance Test Team (EPT). When performance testing is conducted, EPT will provide slides to insert for performance test results.]

14

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 14:
Slide 14 provides a description of performance test results. The IPT should contact the Technology Office, Enterprise Performance Test Team (EPT) to complete this slide. The EPT Team will provide a completed slide to insert at this point in the presentation.

User Acceptance Test Results

Open Defects: [note: FSA generally does not implement releases with open urgent or high defects]

- Medium: [provide description of the defect and the business functionality impacted by the defect]
- Low: [provide description of the defect and the business functionality impacted by the defect]

Closed Defects: [note: only provide urgent and high for closed defects]

- Urgent: [provide description of the defect and the business functionality impacted by the defect]
- High: [provide description of the defect and the business functionality impacted by the defect]

15

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 15:
Slide 15 includes a description of open defects as well as the closed urgent and high severity defects that were encountered during user acceptance testing. All open defects should be explained on this slide. Urgent and High defects that were encountered during testing should also be explained briefly. In general, releases will not be approved at the PRR with urgent or high severity defects that are still open. If an exception to this is needed, please consult with the Enterprise Testing Team prior to the PRR to review the particular situation.

Data Center Readiness

- This release will be implemented in FSA's Virtual Data Center in Plano, TX. [identify other data center if applicable]
- Operational roles and responsibilities between different teams (data center, middleware, application support) have been defined and communicated.
- CMDB review and validation completed on [date – usually done in conjunction with SDR, if release does not have an SDR this validation still needs to be done].
- Service Delivery Review (SDR) completed on [date]. [Describe any outstanding issues from SDR].
- Disaster recovery objectives revalidated based on this release:
  - Recovery Time Objective (RTO): [Mission Essential = 48 hours or Essential = 72 hours or Non-Essential = 72 hours]
  - Recovery Point Objective (RPO): [Mission Essential = 24 hours or Essential = 24 hours or Non-Essential = 48 hours]

16

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 16:

Slide 16 covers the readiness of the data center to support the release or infrastructure change. For releases at the VDC that have a SDR, the SDR will cover most of the information on these slides. The disaster recovery objectives should match the information that is on file with the data center and documented in the system's security documentation. Process steps for CMDB review and update are covered in Steps 9 and 12 of Section 3 in this document.

Data Center Readiness

- Change Request (CCM Ticket) for production implementation has been submitted to the data center. Ticket # [insert ticket number].
- The release will be implemented [during / outside of] the normal maintenance window [state outage period if outside of maintenance window].
- Hour-by-Hour Plan has been completed and all resources understand the actions required to complete implementation.
- Roll-back Plan can be completed within the maintenance window [if extension would be required, indicate how long]

17

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 17:
Slides 17 covers the specific data center change requests that will be implemented in support of the release. This slide also covers the timing of those changes (if the changes can be implemented during the standard maintenance window). If an extension of the maintenance window is needed, that is addressed on this slide.

Data Center Readiness

- A roll-back of this release will occur if [insert specific criteria for when a roll-back would occur]
- [describe the Roll-back Plan - would the previous code base be installed, would a backup be restored, etc.]
- The decision to execute the roll-back plan will be made by the technical team implementing the release based on the criteria described in this PRR, with approval from the System Owner and VDC Manager.

18

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 18:
Slide 18 covers details of the roll-back plan should it be needed. This slide should identify specific criteria for the conditions when a roll-back plan will be activated. The goal of this slide is to communicate the roll-back criteria to all stakeholders in advance of implementation; if those roll-back criteria are met during implementation activities, then the team will know that they should roll-back the release and re-plan the implementation. This advance planning prevents confusion and indecision during implementation activities.

EBC/SharePoint Coordination

- This release is being implemented in the [Employee Enterprise Business Collaboration (EEBC) or Partner Enterprise Business Collaboration (PEBC)] Production Environment.
- This release is a [sandboxed or farm] solution.
- The EBC component(s) used by this release include [MS SharePoint, Serena, K2, etc.]
- [Provide a high-level description of any custom development done as part of this release. For example: This release uses out-of-the-box MS SharePoint features for most functions; however, two pages were customized with Java code to support specific business requirements related to advanced search features in the database.]
- This release was approved by the EBC Change Control Board on [date].
- [Name] is the EBC Change Control Board Representative for this application.

[Note: This slide only applies to releases in the EEBC and PEBC SharePoint environments. If the release covered by the PRR is not being implemented in EEBC or PEBC, then please remove this slide.]

19

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 19:
Slide 19 covers items that are specific to FSA's SharePoint environments (EEBC and PEBC). This slide is required for all releases that use the EEBC and PEBC environments and should be removed for all other releases.

The following paragraph provides additional information for the sandbox or farm determination. A Microsoft SharePoint Server 2010 *solution* is a deployable, reusable package that can contain features, site definitions, and other functionality. Solutions can be enabled or disabled individually. You can deploy a solution directly onto your SharePoint Server farm, or you can deploy the solution into a *sandbox*. A sandbox is a restricted execution environment that enables programs to access only certain resources, and that keeps problems that occur in the sandbox from affecting the rest of the server environment. Solutions that you deploy into a sandbox, which are known as *sandboxed solutions*, cannot use certain computer and network resources, and cannot access content outside the site collection they are deployed in.

Security and Privacy

- Documented system owner is [name]
- ISSO is [name], confirmed by assignment memo dated [date]
- Alternate ISSO is [name], confirmed by assignment memo dated [date]
- System is classified as a [GSS, Major Application, Minor Application]
- System [does/does not] contain Personally Identifiable Information (PII).
- Confidentiality is categorized as [High, Moderate, Low]
- Integrity is categorized as [High, Moderate, Low]
- Availability is categorized as [High, Moderate, Low]

20

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 20:
Slide 20 revalidates the basic security information for the system, including the name of the system owner, name of the ISSO, name of Alternate ISSO, FISMA classification (GSS, Major Application, Minor Application), if the system contains PII data, and the categorizations for confidentiality, integrity, and availability (High, Moderate, or Low). The information on this slide should match the 'Systems' screen under the 'System Inventory' Menu in OVMS.

Security and Privacy

- The System Owner and ISSO [have / have not] reviewed the security and privacy documents on the PRR slides titled "Documentation needed for Implementation and Operations" and verify that all appropriate updates have occurred.
- The ISSO has reviewed the website(s) for the system and validated that a Human and Machine Readable Privacy Policy [is / is not] in place. [if not in place, please explain]
- The ISSO has evaluated the changes being implemented in this release and has determined that there [is / is not] an impact to the security posture/controls of the system [state the impact if there is one].
- The ISSO has validated that a current Authority to Operate (ATO) is in place for the system.
- The Monthly Authenticated Vulnerability Scans are scheduled for the system on [date; i.e. 5th calendar day of month, second Saturday of month, etc.].

21

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 21:

This slide revalidates the security privacy documentation for the system website privacy policy review based on the changes being implemented with the release. This slide also covers the evaluation of changes relative to the security posture of the system and revalidates that the ATO for the system is current. The scheduled date for the Monthly Authenticated Vulnerability scans is included to ensure that teams have coordinated with VDC Security to set up a date each month where the system is scanned as part of continuous scanning activities.

Security Vulnerability Scans

Security Scan Coordination for this release

Scans occurring before PRR	Scan Tool(s)	Actual Date
Application Scan of Development, Test, Stage		
Database Scan of Development, Test, Stage		
Operating System / Infrastructure Scan of Development, Test, Stage		

Scans occurring after PRR	Scan Tool(s)	Actual Date
Application Scan of Production		
Database Scan of Production		
Operating System / Infrastructure Scan of Production		

22

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 22:
Slide 22 addresses which security vulnerability scans have been run in support of this release and that the scans occurred. It also addresses when security scans will be run for the production environment after implementation.

Security Vulnerability Scans

Application Scan results identified by Cyber Security

	Critical	High	Medium
Scan Results addressed by Corrective Action Plan (CAP) – Pending Resolution			
Scan Results addressed by approved Accepted Risk (AR)			
New scan findings entered in OVMS from this scan*			
Total (excludes low severity, informational, and false positive scan results)			

*Details of new scan findings entered in OVMS are addressed on the next slide.

23

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 23:
This slide addresses the results of application vulnerability scans. Based on the analysis from the Cyber Security Team, the ISSO reports the counts of scan results that already have an active Corrective Action Plan (CAP) in place, scan results that have a current and approved Accepted Risk Acceptance (AR) in place, and any new findings that were entered in OVMS for tracking as a result of this scan.

Security Vulnerability Scans

Resolution of New **Application** Scan Findings by ISSO

OVMS ID	Severity Level (Critical, High, Medium)*	Description of Finding	Responsible ISSO (Name)	Mitigation Strategy (CAP or AR)

*Severity Level as reported on previous slide.

24

Federal Student Aid An OFFICE of the U.S. DEPARTMENT of EDUCATION | PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 24:
This slide provides the details on new OVMS entries related to the application vulnerability scan findings. If a scan finding does not have an existing CAP or AR, it must be entered in OVMS for tracking purposes.

Security Vulnerability Scans

Database Scan results identified by Cyber Security

	Critical	High	Medium
Scan Results addressed by Corrective Action Plan (CAP) – Pending Resolution			
Scan Results addressed by approved Accepted Risk (AR)			
New scan findings entered in OVMS from this scan*			
Total (excludes low severity, informational, and false positive scan results)			

*Details of new scan findings entered in OVMS are addressed on the next slide.

25

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 25:
This slide addresses the results of database vulnerability scans. Based on the analysis from the Cyber Security Team, the ISSO reports the counts of scan results that already have an active Corrective Action Plan (CAP) in place, scan results that have a current and approved Accepted Risk Acceptance (AR) in place, and any new findings that were entered in OVMS for tracking as a result of this scan.

Security Vulnerability Scans

Resolution of New **Database** Scan Findings by ISSO

OVMS ID	Severity Level (Critical, High, Medium)*	Description of Finding	Responsible ISSO (Name)	Mitigation Strategy (CAP or AR)

*Severity Level as reported on previous slide.

26

Federal Student Aid An OFFICE of the U.S. DEPARTMENT of EDUCATION | PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 26:
This slide provides the details on new OVMS entries related to the database vulnerability scan findings. If a scan finding does not have an existing CAP or AR, it must be entered in OVMS for tracking purposes.

Security Vulnerability Scans

Infrastructure and Operating System Scan results identified by Cyber Security

	Critical	High	Medium
Scan Results Addressed by Previous Corrective Action Plan – Pending Resolution			
Scan Results Addressed by approved Risk Acceptance			
New scan findings entered in OVMS from this scan*			
Total (excludes low severity, informational, and false positive scan results)			

*Details of new scan findings entered in OVMS are addressed on the next slide.

27

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 27:
This slide addresses the results of infrastructure and operating system vulnerability scans. Based on the analysis from the Cyber Security Team, the ISSO reports the counts of scan results that already have an active Corrective Action Plan (CAP) in place, scan results that have a current and approved Accepted Risk Acceptance (AR) in place, and any new findings that were entered in OVMS for tracking as a result of this scan.

Security Vulnerability Scans

Resolution of New **Infrastructure** Scan Findings by ISSO

OVMS ID	Severity Level (Critical, High, Medium)*	Description of Finding	Responsible ISSO (Name)	Mitigation Strategy (CAP or AR)

*Severity Level as reported on previous slide.

28

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 28:
This slide provides the details on new OVMS entries related to the infrastructure and operating system vulnerability scan findings. If a scan finding does not have an existing CAP or AR, it must be entered in OVMS for tracking purposes.

Configuration Management

Configuration Management Activities:

- [Describe the activities performed by the development organization's configuration management function]

Functional Configuration Audit (FCA):

- [Describe the results of the FCA]

Physical Configuration Audit (PCA):

- [Describe the results of the PCA]

Release Version Description Document (VDD)

- [Describe if a Release Version Description Document was produced for this release; cite date of completion]

Note: Technology Office Configuration Management Team does not perform configuration audits on FSA Major Applications where a third-party developer performs software engineering activities.

29

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 29:

This slide addresses the status of configuration management activities and audits that were performed in support of the release. The configuration manager for the system should provide information on the status of these activities and audits.

Documentation needed for Implementation and Operations

Ent. WBS Code	Document or Work Package from LMM Tailoring Plan dated [MM/DD/YYYY]	Status - Created Document - Updated Existing Doc. - Part of Another Doc. - No update needed - Not applicable to this release	Document Version Number of Final Accepted Document	Date of Final Accepted Document	Comments (If included in another LMM Document, indicate the name of that document and LMM Tailoring Plan Item #.)
1.1.1	Investment Request	[fill in document status from choices above]	[version #]	[date]	[comments]
1.1.2	Business Case/Exhibit 300	[document status]	[version #]	[date]	[comments]
1.1.3	Project Charter	[document status]	[version #]	[date]	[comments]
1.2.1	Lifecycle Management Methodology (LMM) Work Breakdown Structure Dictionary and Tailoring Plan	[document status]	[version #]	[date]	[comments]
3.1	Information System Security Officer (ISSO) Appointment Letter	[document status]	[version #]	[date]	[comments]
3.2.1	Privacy Threshold Analysis	[document status]	[version #]	[date]	[comments]
3.2.2	Privacy Impact Assessment	[document status]	[version #]	[date]	[comments]
3.2.3	System of Records Notice (SORN)	[document status]	[version #]	[date]	[comments]
3.3.1	Memorandum of Understanding	[document status]	[version #]	[date]	[comments]
3.3.2	Computer Matching Agreement	[document status]	[version #]	[date]	[comments]
3.3.3	Interconnection Security Agreement (ISA)	[document status]	[version #]	[date]	[comments]

30

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slides 30-33:

The documentation slides address the status of the system documentation that is needed for implementation of the system and ongoing operations once implemented. Some of the documents are managed at a system level and others apply to each release. For releases (projects) that have completed an LMM Tailoring Plan, the updates on these documentation slides should match the LMM Tailoring Plan. If the LMM Tailoring Plan indicates that a document does not apply, then the document should be marked as “Not applicable to this release” and the comments column should reference the LMM Tailoring Plan.

Documentation needed for Implementation and Operations

Ent. WBS Code	Document or Work Package from LMM Tailoring Plan dated [MM/DD/YYYY]	Status - Created Document - Updated Existing Doc. - Part of Another Doc. - No update needed - Not applicable to this release	Document Version Number of Final Accepted Document	Date of Final Accepted Document	Comments (If included in another LMM Document, indicate the name of that document and LMM Tailoring Plan Item #.)
3.4.1	Business Impact Analysis (BIA)	[fill in document status from choices above]	[version #]	[date]	[comments]
3.4.2	Information Technology (IT) Contingency Plan (Includes Test Plan)	[document status]	[version #]	[date]	[comments]
3.5.1	Data Sensitivity Worksheet	[document status]	[version #]	[date]	[comments]
3.5.2	System Authorization Boundary	[document status]	[version #]	[date]	[comments]
3.5.3	System Security Plan	[document status]	[version #]	[date]	[comments]
3.7	Authority To Operate Letter and Briefing	[document status]	[version #]	[date]	[comments]
3.9	Data Retention Schedule	[document status]	[version #]	[date]	[comments]
4.2	Requirements Management Plan	[document status]	[version #]	[date]	[comments]
4.5	Detailed Requirements Document	[document status]	[version #]	[date]	[comments]
4.6	Requirements Traceability Matrix	[document status]	[version #]	[date]	[comments]

31

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slides 30-33:

The documentation slides address the status of the system documentation that is needed for implementation of the system and ongoing operations once implemented. Some of the documents are managed at a system level and others apply to each release. For releases (projects) that have completed an LMM Tailoring Plan, the updates on these documentation slides should match the LMM Tailoring Plan. If the LMM Tailoring Plan indicates that a document does not apply, then the document should be marked as “Not applicable to this release” and the comments column should reference the LMM Tailoring Plan.

Documentation needed for Implementation and Operations

Ent. WBS Code	Document or Work Package from LMM Tailoring Plan dated [MM/DD/YYYY]	Status - Created Document - Updated Existing Doc. - Part of Another Doc. - No update needed - Not applicable to this release	Document Version Number of Final Accepted Document	Date of Final Accepted Document	Comments (If included in another LMM Document, indicate the name of that document and LMM Tailoring Plan Item #.)
4.7	Data Migration Plan	[fill in document status from choices above]	[version #]	[date]	[comments]
5.1	Configuration Management Plan	[document status]	[version #]	[date]	[comments]
5.3	Detailed Design Document	[document status]	[version #]	[date]	[comments]
5.4	Solution Source Code and Deployable Packages	[document status]	[version #]	[date]	[comments]
5.5	Solution User Manual	[document status]	[version #]	[date]	[comments]
5.6	Release Version Description Document	[document status]	[version #]	[date]	[comments]
6.1	Master Test Plan	[document status]	[version #]	[date]	[comments]
6.2	Test Suites	[document status]	[version #]	[date]	[comments]
6.3.1	User Acceptance Test Summary Report	[document status]	[version #]	[date]	[comments]
6.3.2	System Test Summary Report	[document status]	[version #]	[date]	[comments]

32

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slides 30-33:

The documentation slides address the status of the system documentation that is needed for implementation of the system and ongoing operations once implemented. Some of the documents are managed at a system level and others apply to each release. For releases (projects) that have completed an LMM Tailoring Plan, the updates on these documentation slides should match the LMM Tailoring Plan. If the LMM Tailoring Plan indicates that a document does not apply, then the document should be marked as “Not applicable to this release” and the comments column should reference the LMM Tailoring Plan.

Documentation needed for Implementation and Operations

Ent. WBS Code	Document or Work Package from LMM Tailoring Plan dated [MM/DD/YYYY]	Status - Created Document - Updated Existing Doc. - Part of Another Doc. - No update needed - Not applicable to this release	Document Version Number of Final Accepted Document	Date of Final Accepted Document	Comments (If included in another LMM Document, indicate the name of that document and LMM Tailoring Plan Item #.)
6.3.3	Defect Management Report	[fill in document status from choices above]	[version #]	[date]	[comments]
7.1.1	Implementation Plan	[document status]	[version #]	[date]	[comments]
7.1.2	Transition Management Plan	[document status]	[version #]	[date]	[comments]
7.2	Training Plan	[document status]	[version #]	[date]	[comments]
7.3	Operations and Maintenance Plan	[document status]	[version #]	[date]	[comments]

33

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slides 30-33:

The documentation slides address the status of the system documentation that is needed for implementation of the system and ongoing operations once implemented. Some of the documents are managed at a system level and others apply to each release. For releases (projects) that have completed an LMM Tailoring Plan, the updates on these documentation slides should match the LMM Tailoring Plan. If the LMM Tailoring Plan indicates that a document does not apply, then the document should be marked as “Not applicable to this release” and the comments column should reference the LMM Tailoring Plan.

End User Support and Communication

- Outage window for end users will be [date/time] to [date/time].
- [describe how end users will be notified of the release]
- Application help desk is aware of the release and has updated their procedures. The help desk phone number is [phone number]
- Call center scripts and procedures have been updated to support calls from end users. The Customer Call Center phone number is [phone number].
- [describe any additional end user support / communication activities]

34

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 34:
This slide describes the support and communication to end users. The expected outage window for the application is identified, help desk and call center information is included, and a description of how end users will be notified of the release is provided. Creating or updating a user guide and training activities are also examples of communication that may be addressed on this slide, if that is part of the communication strategy being followed by the release/project.

Lessons Learned

- [Describe how lessons learned were captured for this release.]
- A lessons learned meeting [is/is not] planned for [date/if not planned, explain approach for eliciting lessons].
- Lessons Learned for this release will be entered in FSA's Lessons Learned Database on or before [date].

[Note: This slide should inform readers of the process for identifying and capturing lessons learned. It should not include the specific lessons.]

35

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 35:
This slide describes the process that the project is using for identifying lessons learned. This slide also describes how the lessons learned will be captured and maintained. Federal Student Aid has established a Lessons Learned Database for teams to enter lessons learned and share those lessons across the enterprise; this resource is available to all Federal Student Aid projects for maintenance of lessons learned. Contact the Technology Office, Enterprise Quality Assurance Team for further information on the Lessons Learned Database.

Meeting Closure

- Implementation is scheduled for [date].
- Completion of formal sign-off (next page)
- Delivery of sign-off pages and supporting documentation to Technology Office, Enterprise Quality Assurance Team.

36

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 36:
This slide closes the PRR meeting and reiterates the implementation date for the release or infrastructure change. The sign-off documentation is maintained in the IPT's files and a copy is kept on file by the Technology Office, Enterprise Quality Assurance Team.

PRR Approval (Page 1 of 2)

Federal Student Aid approves implementation of **[System / Release Name and Version]** on **[implementation date]** based on the information included in this Production Readiness Review.

[Name] *Release Project Manager*	[Name] *System Technical Lead*
[Name] *Test Lead*	[Name] *Information System Security Officer*
[Name] *System Owner*	[Name] *Application / Business Owner*
Slawko Semaszczuk, Sanjay Gupta, Wanda Broadus, or designee *Virtual Data Center*	Cheng Tang, Anamaria Matos, Bob Ingwalson or designee *FSA Chief Information Security Officer*

37

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 37:

This slide is the first of two sign-off pages for the PRR. Signatures from the project manager, system technical lead; test lead, ISSO, system owner, application/business owner, Virtual Data Center Manager, and Chief Information Security Officer are obtained on this page.

PRR Approval (Page 2 of 2)

Federal Student Aid approves implementation of **[System / Release Name and Version]** on **[implementation date]** based on the information included in this Production Readiness Review.

Mike Rockis, Trey Wiesenburg, or designee
Enterprise Quality Assurance Program

Sandy England, Jim McMahon,
Ganesh Reddy, Leslie Willoughby or designee
Technology Office Management

Based on the operational risk associated with implementation of this release, sign-off by FSA Senior Management may be required as indicated below. Factors considered in determining operational risk include system criticality, end-user type and volume, release complexity, release size, technology used by the release, implementation team maturity, and timing of the release implementation within the business cycle.

Determination by Enterprise Quality Assurance Program:

- ❑ Senior Management Sign-off is required.
- ❑ Senior Management Sign-off is not required.

[Name of Operating Committee Member]
[Title of Operating Committee Member]

Richard Gordon or designee
FSA Chief Information Officer

38

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND™

Guidance for Slide 38:

This slide is the second of two sign-off pages for the PRR. Signatures from the Enterprise Quality Assurance Program and the Technology Office Management are obtained. In addition, based on the operational risk factors for the release, the Enterprise Quality Assurance will indicate if additional sign-off by FSA Senior Management is required, including the Operating Committee Member responsible for the release and FSA's Chief Information Officer.

Section 5. Sign-Off Responsibilities

There are several individuals who are required to sign-off on a PRR to provide formal approval for the system release or infrastructure change to move in to Federal Student Aid's production environment. The roles for these individuals follow:

Release Project Manager - The Project Manager's signature certifies that the project has produced a complete product and that product is ready to be implemented in the production environment.

System Technical Lead/System Manager - The System Technical Lead/System Manager's signature certifies that all reasonable due diligence has been exercised to ensure system stability/operability, that known risks have been identified/described in the presentation, and that testing has been performed.

Test Lead - The Test Lead's signature certifies that test results have been accurately reported at the PRR and there are no known outstanding test defects that will adversely impact the system or end-users.

Information System Security Officer - The Information System Security Officer's signature certifies that all reasonable due diligence has been exercised to ensure system security, and known risks have been identified/described in the presentation and in the security documentation.

System Owner - The system owner's signature certifies that all reasonable due diligence has been exercised to ensure system stability/operability, that known risks have been identified/described in the presentation, and that a business benefit will be realized by the implementation of the system release or infrastructure change.

Application Owner - The application owner's signature certifies acceptance of business risks associated with implementation of the system or release. This specifically includes the risk of exposing the system or release to end users, including the public for certain releases.

FSA's Chief Information Security Officer – The CISO's signature certifies that the system has received (or is covered by an) authority to operate and has completed all security and privacy documentation that is needed prior to the release entering production. Additionally, the CISO certifies that security vulnerability scan results have been adequately analyzed, remediated, and acknowledged.

Virtual Data Center Manager - The VDC Manager's signature certifies that all VDC issues and concerns have been addressed and the VDC is ready to accept the system into the production environment.

Enterprise Quality Assurance Program - The Enterprise Quality Assurance Program Manager's signature certifies that the PRR was conducted in accordance with Federal Student Aid's PRR Process Standards. If an IV&V vendor participated in the development project, the signature indicates that independent quality assurance activities were performed according to

Federal Student Aid Standards and that the findings identified by IV&V are described in the presentation/supporting documentation.

Technology Office Management – The signature for Technology Office Management certifies that any issues raised by Technology Office program areas have been addressed or there are appropriate mitigation strategies in place to address outstanding issues.

Operating Committee Member responsible for release (if required) - The Operating Committee Member's signature certifies that all reasonable due diligence has been exercised to assure system stability and operability, and that risks identified and described in the presentation/supporting documentation are reasonable given the expected business benefit. The Operating Committee Member's signature also certifies that Federal Student Aid senior management is aware of the release date and associated impacts to Federal Student Aid's end users.

Federal Student Aid's CIO (if required) - The Federal Student Aid CIO's signature certifies that all reasonable due diligence has been exercised to assure system stability and operability, and that risks identified and described in the presentation/supporting documentation are reasonable given the expected business benefit. The CIO's signature also certifies that the implementation of the system component or release is in alignment with Federal Student Aid's strategy for alignment of information technology investments, as required by the Clinger-Cohen Act.

Appendix A – Acronyms and Abbreviations

Appendix A - Acronyms and Abbreviations

ACS	Administrative Communications Systems
ATG	Assistive Technology Group
ATO	Authorization to Operate
BIA	Business Impact Assessment
C&A	Certification & Accreditation
CAP	Corrective Action Plan
CCM	Change Control Management (ticket)
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
COO	Chief Operating Officer
COR	Contracting Officer Representative
COTR	Contracting Officer Technical Representative
COTS	Commercial-off-the-Shelf
CISO	Chief Information Security Officer
ED	Department of Education
ED OCIO	Department of Education, Office of the Chief Information Officer
EEBC	Enterprise Employee Business Collaboration
EIT	Electronic and Information Technology
EOCM	Enterprise Operations Change Management
EPT	Enterprise Performance Test
EQA	Enterprise Quality Assurance
FCA	Functional Configuration Audit
FIPS	Federal Information Processing Standard
G.A.	Guarantee Agency
GAO	General Accounting Office
GPRA	Government Performance and Results Act of 1993
GSS	General Support System
IATO	Interim Approval to Operate

IEEE	Institute of Electrical and Electronics Engineers
IPC	Investment Planning Council
IPT	Integrated Project Team
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
IST	Inter-System Testing
IT	Information Technology
ITIM	Information Technology Investment Management
IV&V	Independent Verification & Validation
LCM	Life Cycle Management (ED)
LMM	Lifecycle Management Methodology (FSA)
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management & Budget
ORR	Operational Readiness Review
OVMS	Operational Vulnerability Management Solution
PCA	Physical Configuration Audit
PEBC	Partner Enterprise Business Collaboration
PIR	Post-Implementation Review
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PRR	Production Readiness Review
QA	Quality Assurance
RACI	Responsibility, Accountability, Communication, Informed
RAF	Risk Acceptance Form
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDR	Service Delivery Review
SLA	Service Level Agreement
SORN	System of Records Notice
SP	Special Publications
SRR	Security Readiness Review

TRR	Test Readiness Review
UAT	User Acceptance Testing
UI	User Interface
VDC	Virtual Data Center
VDD	Version Description Document

Appendix B – Glossary

Appendix B - Glossary

Term	Definition
Business Function	A function that aligns with the mission of the agency (i.e., Loan Consolidation, Reconciliation, Auditing, Business Metric Management).
Common Infrastructure Service(s)	Information resources that provide functionality that is shared with other information resources that exist in multiple systems (i.e., Authentication and Authorization (Security Architecture), WebSphere Application Cluster Server, Oracle DBMS Clusters). (Definition Source: Created by the group in a meeting)
Change Priorities	Emergency - • Correct an application/system halt (abnormal termination) in the production environment • Correct a hazardous condition that may result in injury to personnel or damage to equipment • Effect a change in operational characteristics that, if not accomplished expeditiously, may seriously compromise security or business mission Urgent – • Effect a change that, if not accomplished, may compromise effectiveness, contractual commitments, life cycle costs, or business mission • Correct a condition that is affecting the system or system component that is critical • Effect a change in operational characteristics to implement regulatory requirements with stringent completion date requirements Routine – • Assigned when emergency or urgent implementation is not applicable, required, or justifiable
Information Resource	Information and related resources, such as personnel, equipment, funds and information technology (i.e., Oracle Financials 11i, WebSphere Application server, HP RP5400 Server, Cisco 2900 Series Routers, PIX 500 Series Firewalls). (Definition Source: FIPS 199 02/2004)
Integrated Project Team (IPT)	A cross-functional team consisting of individuals from across the organization that is responsible for delivering a specific product such as software or a system release.
Microsoft SharePoint 2010	A Microsoft SharePoint Server 2010 *solution* is a deployable,

Term	Definition
Solution (Sandbox and Farm Deployments)	reusable package that can contain features, site definitions, and other functionality. Solutions can be enabled or disabled individually. You can deploy a solution directly onto your SharePoint Server farm, or you can deploy the solution into a *sandbox*. A sandbox is a restricted execution environment that enables programs to access only certain resources, and that keeps problems that occur in the sandbox from affecting the rest of the server environment. Solutions that you deploy into a sandbox, which are known as *sandboxed solutions*, cannot use certain computer and network resources, and cannot access content outside the site collection they are deployed in.
Operational Readiness Review (ORR)	Review performed by the IPT (both Federal staff and contractors) that is directly responsible for the development of a release of an information system or system component.
Production Readiness Review (PRR)	Review performed by the Federal Student Aid enterprise to ensure that a release of an information system or system component will perform as intended in the production environment and that the release meets Federal government requirements for information systems.
System (i.e., information system)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposal of information. (Definition Source: FIPS 199 02/2004)
System Component	A functional unit that publishes and/or processes information with an independent software code base that provides specific functionality for a system that is produced through a software development process or commercial-off-the-shelf (COTS) implementation. (Definition Source: Created by the group in a meeting)
System Release Types	Major: a significant change in the functionality or technical characteristics of the system or a system component. Typically, there is 50% or more change to the configuration items or significant new functionality has been added; whole number version increments, which also includes operating system and software upgrades. Minor: a less significant functional or technical change. Typically, less than 50% of configuration items will have been changed and no new major functionality will have been added. Also applies to operating system and software upgrades that are less than whole number version increments. Patch: a change to fix a deficiency in the controlled item with no new functionality added.