

# **Production Readiness Review (PRR) Process Description**

**Version 16.0**

**FINAL**

**July 29, 2016**

**Document Identifier: FSA\_TOQA\_PROC\_RLS.PRR\_001**

## Document Version Control

Version	Date	Description
16.0	7/29/2016	<ul style="list-style-type: none"> <li>• Presentation Template Updates:               <ol style="list-style-type: none"> <li>1. Removed slide related to EBC/SharePoint-specific items; this information is generally covered in the main PRR so there is no longer a need for this slide.</li> <li>2. Added “Review of Open Issues” slide to distinguish between risks and issues being reported at the PRR.</li> <li>3. Added FSA Employee Impact (labor relations review) item to the Scope of Release slide.</li> <li>4. Added LMM Tailoring Plan status item to the LMM Technical Stage Gates slide.</li> <li>5. Divided slides previously titled “Documentation needed for Implementation and Operations” into three areas: Security Documentation, System Documentation, and Release Documentation and enhanced guidance on reporting the status of the documents.</li> <li>6. Updated OVMS References to a generic tool reference in anticipation of CSAM migration.</li> <li>7. Minor enhancements to guidance throughout the document.</li> </ol> </li> <li>• Conforming updates and minor guidance enhancements in this document to support the template changes described above.</li> </ul>
8.0 - 15.1	9/30/2015	For previous revision history of Versions 8.0-15.1, see Version 15.1.
1.0 - 7.0	6/19/2007	For previous revision history of Versions 1.0-7.0, see Version 7.0

## Table of Contents

<b>DOCUMENT VERSION CONTROL</b> .....	<b>I</b>
<b>TABLE OF CONTENTS</b> .....	<b>II</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>1</b>
<b>SECTION 1. INTRODUCTION</b> .....	<b>2</b>
1.1 Purpose.....	2
1.2 Intended Audience .....	2
1.3 Document Organization .....	3
1.4 References and Related Documents .....	3
<b>SECTION 2. RISK-BASED CRITERIA FOR CONDUCTING A PRR</b> .....	<b>5</b>
<b>SECTION 3. PRR PROCESS</b> .....	<b>7</b>
Step 1: LMM Tailoring Plan.....	9
Step 2: Requirements, Design, Development, and Testing Activities.....	9
Step 3: Release Request Created .....	10
Step 4: Schedule Pre-PRR and PRR .....	10
Step 5: Reviews by Technology Office Support Areas .....	10
Step 6: Internal IPT Readiness Review .....	11
Step 7: Draft PRR Presentation Distributed .....	12
Step 8: Pre-PRR .....	12
Step 9: Service Delivery Review (SDR).....	12
Step 10: PRR Presentation Distributed .....	13
Step 11: PRR Presentation and Sign-off.....	13
Step 12: Release Production Implementation .....	13
<b>SECTION 4. PRR PRESENTATION</b> .....	<b>15</b>
<b>SECTION 5. SIGN-OFF RESPONSIBILITIES</b> .....	<b>52</b>
<b>APPENDIX A - ACRONYMS AND ABBREVIATIONS</b> .....	<b>55</b>
<b>APPENDIX B - GLOSSARY</b> .....	<b>59</b>

## Executive Summary

The Production Readiness Review (PRR) Process is a quality review of system releases and infrastructure changes 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 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. There are several key activities that must be completed prior to the PRR, these include completion of all test phases, completion of the hosting data center review when required, security scans, review of security posture/control impacts, and release-related documentation updates.

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, 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 FSA enterprise-level 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 and approval 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 and are completed 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 Aid 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

The 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 1.3, June 30, 2015.
- LMM Stage Gate Process Description, Federal Student Aid, Version 1.3, June 30, 2015.
- Enterprise Change Management Plan, Version 2.1, Federal Student Aid, June 5, 2014.
- Cyber Security Vulnerability Analysis (VSA) Standard Operating Procedure (SOP), Version 11.7, Federal Student Aid, July 31, 2015.
- 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 4.0.1, Federal Student Aid, September 30, 2013.
- 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 4, *Recommended Security Controls for Federal Information Systems and Organizations*, NIST, April 2013

## 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 Technical Review Board (TRB) and 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.

Operational risks must be considered for all changes. A systematic process will be used for identifying, analyzing, and assigning risk that a release's impact will have on IT services or systems operations, the system, the system's purpose (mission), or FSA's mission. The TRB will initially evaluate the release and recommend the risk rating. The ECCB will then review the risk rating, as part of a release request, and approve the release request.

The risk ratings are high, medium, and low and are based on seven categories. The categories assess the maturity of the system and support staff as well as the importance of the system to FSA. The categories are as follows:

1. System Criticality – system is categorized as Mission Essential, Essential, or Non-Essential.
2. System End User Type and Volume – external or internal to FSA and the volume/audience impacted
3. Interfaces – Number of interfacing systems that will be impacted by the release (this includes any system that has to perform intersystem testing)
4. 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)
5. Technology – new to the market or FSA's operating environment, or out-of-support
6. Maturity –support organization's time and experience in supporting system
7. 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.

To obtain a risk rating, a release will be evaluated using the information in the table below. For categories 3-7, if a single item falls into the higher category, then the higher risk rating is used. If category 2 is the only category listed as high (i.e. a fairly insignificant change/release on a system with a large end-user population), then the overall risk may be reduced to medium based on recommendation by the TO/QA and approval by the ECCB.

For additional information regarding meeting times and procedures for the TRB and ECCB, please refer to the Enterprise Change Management (ECM) Plan, TRB and ECCB charters, and procedures documentation produced by the boards.

Category	High	Medium	Low
1. System Criticality	Critical or important	Critical, important, or supportive	Important or supportive
2. 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
3. Interfaces	More than two	One or two	None
4. Size	Major	Minor	Patch
5. 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
6. 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 performed previous releases of this system.
7. 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 ECCB has responsibility for assigning operational risk, which determines the requirement for a PRR. The TRB will make an initial assessment/recommendation of Operational Risk during the weekly TRB meeting. The final approval of Operational Risk is made by the ECCB at their bi-weekly meeting. Operational Risk ratings are documented in the ECM Tool within Rational ClearQuest and in Enterprise Master Release Schedule. Please see the ECM Plan, TRB charter, and ECCB charter for specifics regarding meeting times and representation.

A PRR is not required for an emergency release/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 recommended 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 COR, 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	Release Request created in FSA Enterprise Change Management System	Based on project schedule. 3 – 5 months before release implementation date.  Prefer that this request is opened as soon as project has a realistic implementation date and that release request ticket is updated if implementation dates change. Generally, a release request cannot be opened until requirements for the release are complete.	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	<p>Reviews by Technology Office support areas and ISSO:</p> <ul style="list-style-type: none"> <li>- Enterprise Testing Team (ETT) Reviews Test Results for all phases of testing for projects where manages/supports test efforts.</li> <li>- System Owner and ISSO Security Review</li> <li>- Security Vulnerability Scans conducted</li> <li>- Configuration Management Audits (Functional Configuration Audit and Physical Configuration Audit)</li> </ul>	Based on project schedule. Started before Pre-PRR, must complete before PRR.	<p>IPT</p> <p>Technology Office Support Areas</p>
6	Internal IPT Readiness Review	Based on project schedule. Must occur before Pre-PRR.	IPT
7	Draft of PRR Presentation distributed	T – 16 business days Must occur before Pre-PRR.	IPT
8	Pre-PRR	T – 14 business days	<p>IPT</p> <p>Technology Office</p>
9	<p>Service Delivery Review (SDR) by Data Center Contractor. A review of the Configuration Management Database entries and Application Specific Information (ASI) document are performed as part of the SDR.</p> <p>Note: This step may not be required or may be addressed differently if the system is not hosted at the VDC.</p>	If applicable, SDR must be completed prior to PRR, but can occur after the Pre-PRR. Any outstanding issues from SDR must be reported at PRR.	<p>IPT</p> <p>Virtual Data Center</p>
10	PRR Presentation distributed	T – 8 business days	IPT
11	PRR Presentation and Sign-Off	T – 5 business days	<p>IPT</p> <p>Technology Office</p>
12	Release Production Implementation	T	<p>IPT</p> <p>Technology Office Support Contractors – Application, Middleware, and Data Center</p>

**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, as updated throughout the project, 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)
- IPT Internal Readiness Review 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: Release Request Created**

Once the IPT has completed requirements definition for a release and determined a production implementation schedule, a Release Request should be opened in the FSA Enterprise Change Management Tool (Rational ClearQuest). This request is used across the FSA organization to monitor the planned implementation date of system releases and infrastructure changes. Release 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 Technical Review Board (TRB) and Enterprise Change Control Board (ECCB) based on the release request. In addition, Release Requests are required for scheduling activities for data center change requests and security scans. Therefore, it is critical that this release request be opened as early in the life of a release or infrastructure change as possible.

As part of creating the Release Request, the IPT will be required to submit information regarding all of the LMM Technical Stage Gates for the release/project, including Requirements Review, Preliminary Design Review, Detailed Design Review, Test Readiness Review, PRR, and the Retirement and Disposal Review. The IPT should include the planned dates for each of the Technical Stage Gates and supporting comments; if a particular review does not apply to the release, the target implementation date should be included and the comments should explain why the stage gate does not apply. This information is reported also reported later in the lifecycle, at the PRR on the LMM Technical Stage Gates slide. Please see the Enterprise Change Management (ECM) Release Request (RR) Guidelines document for further information on completing the release request.

### **Step 4: Schedule Pre-PRR and PRR**

The Pre-PRR and PRR meetings should be scheduled after the Release Request has been dispositioned by both the TRB and ECCB (since these boards may change the requirement for holding a PRR); and once the IPT is confident that their development schedule is realistic and finalized. The Pre-PRR should take place approximately 14 business days before the production implementation date and the PRR should take place approximately 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. Support contractors may attend the PRR. Please coordinate with the Enterprise Quality Assurance Team if there is substantial deviation from these timeframes (i.e. a “quick turnaround” PRR is needed).

### **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:

1. 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.
2. The Technology Office Enterprise Performance Test (EPT) Team evaluates each release to determine if performance testing is appropriate by completing a checklist with the IPT for the release. 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. Please note that the EPT Team conducts performance testing on systems located in the VDC; for systems hosted outside the VDC, it may be appropriate for system owners to arrange performance testing through other support contractors.
  3. Security posture review – the ISSO and System Owner 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 IPT.
  4. Security Vulnerability Scanning – the ISSO coordinates vulnerability scanning and analysis, supported by the Technology Office Cyber Security Team. Security Vulnerability Scans are a critical component that is checked at the PRR. The Pre-PRR and PRR (step 7 and after) should not be held with missing or incomplete scan results. Scan results are required to be current within 30 days of the PRR date (scans must have been run no more than 30 days prior to the date of the PRR). FSA’s CISO or CIO may allow a variance (or waiver) of this 30 day requirement.
  5. 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.
  6. 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: Internal IPT Readiness Review

Step 6 of the PRR Process is for the IPT to hold an internal IPT 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. Many teams choose to use the PRR slides as the foundation of this review, but this is at the discretion of the IPT.

## **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 are encouraged to 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 and the invitees in the Pre-PRR should identify any changes needed to complete the PRR Presentation by no later than one business day after the pre-PRR is held. 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.

The system technical lead should review the infrastructure diagram(s) and other information in the Application Specific Information (ASI) document to ensure that all information is still current and up to date. If updates are required, the system technical lead should request that the data center make appropriate updates to ensure that infrastructure diagrams and other information stay current.

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. There is a sign-off page for support contractor management to sign as well as pages for the federal officials approving the release to sign.

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.

In extraordinary and rare cases, the Production Readiness Review and/or sign-off may take place via e-mail. In cases where the PRR presentation is distributed by e-mail, without a formal meeting, prior approval is required by the Technology Office Enterprise Quality Assurance Team; in general, this will only be allowed where there are several similar related PRRs, such as the same infrastructure change being made to multiple systems across different implementation dates. In cases where there is a PRR meeting, but the sign-off is conducted electronically, the Technology Office Enterprise Quality Assurance Team will coordinate the e-mail response process for electronic sign-off; this form of sign-off is the least preferred option and requires prior approval as well.

## **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 Release
3. Schedule Overview
4. Review of Open Issues
5. Review of Open Risks
6. Infrastructure Diagram
7. Testing Activities and Results
8. Enterprise Change Management
9. Data Center Readiness
10. Roll Back Plan
11. Security & Privacy
12. Security Vulnerability Scans
13. Security Documentation
14. Operations and Maintenance
15. End User Support and Communication
16. LMM Tailoring and Technical Stage Gate Completion
17. System Documentation
18. Release Documentation
19. Lessons Learned
20. 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. The PRR is item 7.4 on the LMM site.

Link to LMM Site on EEBC/SharePoint: [LMM SharePoint Library](#)

# Production Readiness Review Presentation Template

Version 16.0  
July 29, 2016

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 implementations and releases; information requested by this template should be included in the presentation in a way that is understandable within the context of the implementation/release.
- Information in [brackets] is to be filled out or provides guidance to be followed. All the brackets and guidance text should be removed from the final 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.
- No item in the PRR should be marked “N/A” or “Not Applicable” unless specified in the guidance; instead an explanation should be provided as to why a particular item does not apply.

**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.

## Reminders:

- Make sure that all text is black throughout the presentation and that all brackets [ ] are removed from the final presentation.
- No item in the PRR should only be marked “N/A” or “Not Applicable;” instead an explanation should be provided as to why a particular item does not apply.



PROUD SPONSOR of  
the AMERICAN MIND™

## [System Name and Version Number]

Production Readiness Review

FSA Release Request Number [Insert RR Number]

[Date]

### 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), the release request number from the ECM system, and the date of the PRR Presentation.

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 Release
3. Infrastructure Diagram
4. Schedule Overview
5. Review of Open Issues
6. Review of Open Risks
7. Testing Activities and Results
8. Enterprise Change Management
9. Data Center Readiness
10. Roll Back Plan
11. Security & Privacy
12. Security Vulnerability Scans
13. Security Documentation
14. Operations and Maintenance
15. End User Support and Communication
16. LMM Tailoring and Technical Stage Gate Completion
17. System Documentation
18. Release Documentation
19. Lessons Learned
20. 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 20 standard agenda items listed in the template and any additional items that the IPT would like to cover at the PRR.

## Business Background of System

[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

[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.]

5

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

PROUD SPONSOR of  
the AMERICAN MIND™

### Guidance for Slide 5:

Slide 5 describes the scope of the specific release. This slide addresses 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.

## Scope of Release

### Business Impact of delaying implementation of this 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.]

### Interfacing/Other FSA Systems impacted by this release:

- [System name – describe impact]
- [System name – describe impact]
- [System name – describe impact]

### FSA employee impact of this release:

A review of this release was completed by the FSA Labor Relations (Human Resources) and it was determined that the changes being implemented in this release do not affect work or employment conditions of any FSA staff.

[Please consult with FSA Labor Relations well in advance of the PRR and determine if the changes included in the release will cause a staff impact.]

6

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

PROUD SPONSOR of  
the AMERICAN MIND™

### Guidance for Slide 6:

Slide 6 describes 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.

This slide also addresses the names and impacts of this release on other interfacing systems at a high level. This information informs the reader that other releases are (or are not) co-dependent on this release.

Lastly, this slide includes a section for the evaluation of how the release impacts FSA employees. Particularly, the system owner needs to consult with FSA Labor Relations (Human Resources) to evaluate the release for changes to work processes and work conditions for federal staff and ensure that appropriate training has been provided to the staff that will be impacted. In some situations, FSA Labor Relations may determine that union negotiations are required prior to implementing a release that has a substantial employee impact. Amandeep Gill and Larra Pleasant are the points of contact in Human Resources.

# Infrastructure Diagram

[Insert a high-level infrastructure diagram for the system.]

For implementations that modify the system infrastructure (i.e. beyond application code changes), please insert two diagrams – one showing the existing infrastructure and one showing the new infrastructure to be implemented.

Systems in FSA’s VDC may use the diagram(s) maintained in the Application Specific Information (ASI) document.

The legend on the infrastructure diagram must include a date that the diagram was produced or is accurate to. The legend must also include the source of the diagram.]

7

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

PROUD SPONSOR of  
the AMERICAN MIND™

## Guidance for Slide 7:

Infrastructure diagrams should be included in the PRR to show the basic layout of the system. It is not necessary to cover every minor detail, but a participant not familiar with FSA operations should get an understanding of the major components of the system from reviewing the infrastructure diagram.

Project Teams may use the same diagram that is presented at the Service Delivery Review in the Application Specific Information (ASI) Document (for VDC systems) or from Security Documentation (such as a system boundary document) to address this requirement. PRRs that include infrastructure changes (such as adding additional servers, virtualization activities, or modifying network connections) should include a “before” and “after” diagram related to the changes, so that PRR reviewers can see the changes that are being made to the infrastructure.

# Schedule Overview

	Planned (baseline) Completion	Actual Completion
Requirements	1/30/2008	2/30/2008
Design	2/30/2008	4/20/2008
Development	5/30/2008	7/30/2008
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
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 (final completion date for all non-prod scan activities)	8/14/2008	10/14/2008
Service Delivery Review (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

Completion dates for LMM Technical Stage Gates are included later in this presentation.

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 covers a high-level review 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.

Schedule items should never be listed as “N/A” or “Not Applicable.” Instead, insert a reference in the date cell, such as “See Explanation - Slide 17” to indicate that there is an explanation of the activity further in the presentation.

Each system that undergoes intersystem testing should be listed on a separate row in the table.

PRRs for infrastructure changes may need to significantly adjust the schedule slide to align with the particular infrastructure activities. Planned (baseline) Completion dates should reflect the dates from the currently approved baseline of the project schedule. If no formal schedule baselines are used, then the development contract dates or the first project schedule produced should be used as the baseline. 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 Issues

<b><u>Open Issues</u></b> related to this implementation/release Definition of Issue: A point or matter in question or in dispute, or a point or matter that is not settled and is under discussion or over which there are opposing views or disagreements. As of the PRR, issues are matters that have occurred and are currently impacting the implementation of the release.			
Issue Description	Issue Resolution Approach	Notes / Comments	Issue Owner
[describe open issue, if none please indicate "No Open Issues" and leave other columns blank. ]	[describe how the issue is being resolved (i.e. a work-around, accepting the impact of the issue, etc). ]	[include any notes or comments that may inform management about this issue]	[Name of Federal Staff Member and their role]

9

**Guidance for Slide 9:**

This slide provides the PRR Participants with a listing of the open issues related to implementing a release or infrastructure change in the production environment. This slide should only cover issues specific to the implementation and immediate production operations of the system. It should not include project issues outside of those that specifically relate to the production implementation. When FSA Management signs-off on the PRR, they are approving implementation even with the issues listed.

Examples of issues may include:

- ATO Still In Progress (management will generally not sign off with this as an open issue)
- Testing Still in Progress (management will generally not sign off with this as an open issue, but there are rare circumstances where it has occurred in the past)
- Training delays
- Weekend data center patching activities impacting the implementation schedule and requiring an extension of the maintenance window to accomplish the release.
- An extended outage for implementation that may impact end users.

If no issues are identified, then the IPT should indicate “No Open Issues” in the first row of the table.



# Review of Open Risks

Open Risks related to this implementation/release					
Definition of Risk: An <b>uncertain event</b> or condition that, if it occurs, has a positive or negative effect on one or more release objectives. Note: If an event has occurred or is a certainty then it becomes an issue rather than a risk.					
Risk Category	Risk Description	Probability	Impact	Mitigation Strategy	Risk Owner
[Ex: Infrastructure]	[Describe Open Risk, if none please indicate "No Risks Identified" and leave other columns blank ]	[High, Moderate, Low]	[High, Moderate, Low]	[Describe strategy that is being used to mitigate the risk in conjunction with the implementation of the release]	[Name of Federal Staff Member and their role]
[Ex: Application Interfaces]					
[Ex: Operations]					

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.



### Guidance for Slide 10:

This slide 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 IPT should identify a category associated with each risk. Some example categories are included in the template. Any category of risk is acceptable, as long as the text of the risk item applies 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.

If no risks are identified, then the IPT should indicate “No Risks Identified” in the first row of the risk table – there are always unknown risks.

# Testing Activities

Test Phase	Organization Executing Tests	Status of Testing
<b>System Testing –</b> 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.]
<b>Intersystem Testing –</b> 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.]
<b>Accessibility (508) Testing –</b> 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.]
<b>Performance testing –</b> 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.]
<b>User Acceptance Testing –</b> 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.]

**Guidance for Slide 11:**

Slide 11 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).

Each system that undergoes intersystem testing should be listed on a separate row in the table. Systems hosted outside of the VDC may indicate a different performance testing team under the “Organization Executing Tests” column on the performance testing row. Please consult with the Technology Office Enterprise Testing Team in completing this slide.



# 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
<b>TOTALS</b>	<b>210</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>80</b>	<b>5</b>	<b>5</b>	<b>5</b>	<b>5</b>	<b>20</b>	<b>5</b>	<b>5</b>	<b>5</b>	<b>5</b>	<b>20</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>40</b>

**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.

**Note: FSA generally does not implement releases with open urgent or high severity defects.**



Guidance for Slide 12:

This slide 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.

Each system that undergoes intersystem testing should be listed on a separate row in the table. Please consult with the Technology Office Enterprise Testing Team in completing this slide.

# System Test Results

System Test Results	Intersystem Test Results
<p>Open Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide description of defect(s) and impact to business functionality]</li> <li>• High: [provide description of defect(s) and impact to business functionality]</li> <li>• Medium: [provide description of defect(s) and impact to business functionality]</li> <li>• Low: [provide description of defect(s) and impact to business functionality]</li> </ul> <p>Closed/Resolved Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide high level description of urgent defects that were closed]</li> <li>• High: [provide high level description of urgent defects that were closed]</li> </ul>	<p>Open Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide description of defect(s) and impact to business functionality]</li> <li>• High: [provide description of defect(s) and impact to business functionality]</li> <li>• Medium: [provide description of defect(s) and impact to business functionality]</li> <li>• Low: [provide description of defect(s) and impact to business functionality]</li> </ul> <p>Closed/Resolved Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide high level description of urgent defects that were closed]</li> <li>• High: [provide high level description of urgent defects that were closed]</li> </ul>

13

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

PROUD SPONSOR of  
the AMERICAN MIND™

Guidance for Slide 13:

This slide includes a description of open defects as well as the closed urgent and high severity defects that were encountered during system testing and 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 (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.

# User Test Results

Accessibility Results	User Acceptance Test Results
<p>Open Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide description of defect(s) and impact to business functionality]</li> <li>• High: [provide description of defect(s) and impact to business functionality]</li> <li>• Medium: [provide description of defect(s) and impact to business functionality]</li> <li>• Low: [provide description of defect(s) and impact to business functionality]</li> </ul> <p>Closed/Resolved Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide high level description of urgent defects that were closed]</li> <li>• High: [provide high level description of urgent defects that were closed]</li> </ul>	<p>Open Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide description of defect(s) and impact to business functionality]</li> <li>• High: [provide description of defect(s) and impact to business functionality]</li> <li>• Medium: [provide description of defect(s) and impact to business functionality]</li> <li>• Low: [provide description of defect(s) and impact to business functionality]</li> </ul> <p>Closed/Resolved Defects:</p> <ul style="list-style-type: none"> <li>• Urgent: [provide high level description of urgent defects that were closed]</li> <li>• High: [provide high level description of urgent defects that were closed]</li> </ul>

14

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

PROUD SPONSOR of  
the AMERICAN MIND™

Guidance for Slide 14:

This slide includes a description of open defects as well as the closed urgent and high severity defects that were encountered during accessibility (508) testing and 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.

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. This slide and the following slide should be replaced with the slides provided by the EPT Team.

The following slide is provided as a format for teams that conduct performance testing internally, rather than through EPT.]

15

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

PROUD SPONSOR of  
the AMERICAN MIND™

## Guidance for Slide 15:

This slide 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. I describe the approach on this slide and complete slide 14.

Systems that are hosted outside the VDC may substitute relevant performance testing slides at this point in the presentation.

# Performance Test Results

Type of Test	Description of Test Performed	Performance Targets	Performance Results
Peak			
Stress			
Perf. Over Time			
Failover			

**Guidance for Slide 16:**

This slide provides a format for reporting the results of performance testing. This format includes listing the type of test performed (Peak, Stress, Performance Over Time, Failover, etc), describing the test that was performed, the performance targets, and the actual performance results that were observed during performance testing.

Systems that are hosted outside the VDC may substitute relevant performance testing slides at this point in the presentation.

# Enterprise Change Management (ECM)

Organizational Need Requests (ONRs) related to this release			
ONR #	Title		
[#####]	[Title]		
	[multiple ONRs may be associated with one release]		
Release Request (RR) for this release			
RR #	Title		
[#####]	[Title] [Typically a PRR covers only one release with only one associated RR]		
VDC Change Requests (VDC CRs) related to this release			
VDC CR #	Title	Environment	State
[#####]	[Title]	[i.e. Production]	[i.e. scheduled]
	[multiple VDC CRs may be linked to a release]		

[Note: For Change Requests (CR) impacting the Virtual Data Center (VDC) affected and configured items, such as infrastructure, system software, middleware, business applications, and network, which reside at the VDC and do not require VDC vendor support, are required to be submitted into the VDC Enterprise Configuration Management (ECM) Tool and labeled by the submitter as an For Your Information "(FYI)" Change Request (CR). The "FYI VDC CR" ticket is required for audits, trouble-shooting incidents, and impact to the VDC contractual SLAs..]

17

**Guidance for Slide 17:**

This slide lists the numbers and titles of requests in the Enterprise Change Management System that are related to the release. This includes ONRs, the RR, and VDC CRs.

## 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.
- 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. The hour-by-hour plan has been distributed to all parties involved, including the 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:

This slide covers the basic data center readiness and coordination associated with the release. This information includes the location of the data center where the release is being implemented, understanding of roles and responsibilities, the implementation window, and coordination of hour-by-hour implementation activities.

**It is extremely important to provide copies of all hour-by-hour plans to the VDC Operations Team so that VDC support can be coordinated in support of system releases.**

For implementations occurring outside of the VDC (i.e. non-VDC data center providers or cloud providers), this slide may be adjusted as needed while covering the same basic information.

## Data Center Readiness

- A Service Delivery Review (SDR) is required by the VDC if a system/system component or infrastructure is added and the VDC provider's support and/or processes are changed. [ This release completed an SDR on [date.] // OR// An SDR was not required for this release because FSA and the VDC provider determined that it did not meet the SDR criteria, as confirmed by e-mail dated [date] from [person]. // OR // If the application is hosted outside of VDC, explain the infrastructure/cloud provider's process for ensuring that they are ready to support FSA's business/application. ]
- Configuration Management Database (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 occur].
- Application Specific Information (ASI) Document, including infrastructure diagram, was last updated on [date].
- 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]

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 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 this slide. The disaster recovery objectives should match the information that is on file with the data center and documented in the system's security documentation. It is expected that each application/system will maintain a current infrastructure diagram (typically part of the ASI document). Process steps for CMDB review and update are covered in Steps 9 and 12 of Section 3 in this document.

For implementations occurring outside of the VDC (i.e. non-VDC data center providers or cloud providers), this slide may be adjusted as needed while covering the same basic information.

## Roll-back Plan

- The Roll-back Plan will be executed if [describe conditions that would cause the release to be rolled back, for example “if production validation testing fails”]
- The Roll-back Plan consists of [describe how release will be rolled back if needed]
- Roll-back Plan can be completed within the maintenance window [if extension would be required, indicate how long]
- 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.

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 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.

# Security and Privacy

- Documented system owner is [name]
- ISSO is [name], confirmed by appointment letter dated [date]
- Alternate ISSO is [name], confirmed by appointment letter dated [date]
- System is classified as a [GSS, Major Application, Minor Application, or a component of one of these categories]
- System [does/does not] contain Personally Identifiable Information (PII). [Provide a summary of the types of data elements for the system]
- Confidentiality is categorized as [High, Moderate, Low]
- Integrity is categorized as [High, Moderate, Low]
- Availability is categorized as [High, Moderate, Low]
- [System name] [does/does not] participate in FSA's Ongoing Security Authorization Program. The ISSO has validated that a current Authority to Operate (ATO) is in place for the system. The most recent ATO [or continuous ATO] was signed on [date].

21

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

PROUD SPONSOR of  
the AMERICAN MIND™

## Guidance for Slide 21:

Slide 21 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 (General Support System (GSS), Major Application, Minor Application), if the system contains PII data, and the categorizations for confidentiality, integrity, and availability (High, Moderate, or Low).

- Please ensure that the slide contents match the CSAM entries, since CSAM will be the official departmental registry for FISMA reportable systems.
- All FSA systems need a designated ISSO and AISSO who is a Federal employee.
- Include PII contained within your system, as stated in your SORN, if applicable.
- All systems are required to move into continuous monitoring. If your system does not currently participate in OSA, then please include a date for compliance and ensure an existing POAM id# for reference.

## Security and Privacy

- The System Owner and ISSO have evaluated the changes being implemented in this release and have 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 verified this release [does/does not] involve the collection of any new data elements or data collection from new data subjects, and that this release [does/does not] involve the sharing of data with new business partners. [state the new data/partners if applicable]
- The System Owner and ISSO [have / have not] reviewed the documents on the PRR slide titled "Security Documentation" 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]
- In accordance with OMB M-15-13 and NIST 800-52, the System Owner and ISSO confirm that all websites and services provided by this system [are available only through a secure connection (HTTPS) //OR// have a plan in place to utilize secure connections (HTTPS) by December 31, 2016.]
- The Monthly Authenticated Vulnerability Scans are scheduled for the system on [date; i.e. 5<sup>th</sup> calendar day of month, second Saturday of month, etc.].

22

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

PROUD SPONSOR of  
the AMERICAN MIND™

### Guidance for Slide 22:

This slide revalidates the security privacy documentation for the system and 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. On the third bullet, system owners and ISSOs are encouraged to review OMB's Guidance in M-15-13 and report on the status of migrating systems to utilizing secure connections via HTTPS and TLS. 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.

- Please evaluate the security impact from changes occurring during the scope of this project. Include an impact statement if there are significant changes to the security posture of the system and/or new data elements being collected.
- Please review the documentation requirements and update the bullet and chart (on the next slide).
- All systems are scanned regularly. Please include the scheduled date(s) on the last bullet of this slide, e.g., "15<sup>th</sup> of each month" or "2<sup>nd</sup> Sunday of each month".

[most recent version and update date should be identified in the table below, but updates are only needed on condition changes, not necessarily with each release]

# Security Documentation

Ent. WBS Code	Document	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 document, indicate the name of that document)
3.1	Information System Security Officer (ISSO) Appointment Letter	[fill in document status from choices above]	[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]
3.4.1	Business Impact Analysis (BIA)	[document status]	[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]
**	Incident Response Plan	[document status]	[version #]	[date]	[comments]

Guidance for Slide 23:

This slide covers the status of security documentation for the system. The IPT should not modify the Ent. WBS Code or Document columns. The team should use the remaining columns to provide the status, document version, date, and any comments on the document. It is understood that these document do not necessarily update for every release (PRR), but may need to be updated for a particular release. The IPT should be able to explain why documents are updated (or not) based on the scope of the changes that are being implemented and this explanation should be incorporated in the comments column.

# Security Vulnerability Scans

## Security Scan Coordination for this release

Scans occurring before PRR	Scan Tool(s)	Scan Request Date	Scan Completed Date	Analysis Complete Date	Findings Entry Date
Application Scan of Non-Production Environments (Dev, Test, Stage, etc.)					
Database Scan of Non-Production Environments (Dev, Test, Stage, etc.)					
OS/Infrastructure Scan of Non-Production Environments (Dev, Test, Stage, etc.)					

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

24

Guidance for Slide 24:

This slide addresses which security vulnerability scans have been run in support of this release, the timing/sequence of scan activities, and that the scans occurred. It also addresses when security scans will be run for the production environment after implementation.

## Security Vulnerability Summary

	Critical	High	Moderate
New findings resulting from this release/project (New CAP or New AR)	4	0	0
Existing POAMs (Existing CAP or Existing AR)	10	0	0
Total	14	0	0

Note: Validated false positive findings are not included in the counts above and are recorded by the POAM Team and stored on a shared drive for future reference.

**[Guidance:**

- New findings line should contain the number of findings reported on the injection template.
- Existing POAMs line should contain number of findings in the vulnerability management tool. ]

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 security vulnerabilities that have been recorded for the system, both from the current release/project and existing Plans of Actions and Milestones (POAMs) that have already been recorded in the vulnerability management tool.

In order to simplify and to better understand the overall security impact to the system from this release/project, there are two rows to be completed by the ISSO. Using the data from the vulnerability management tool, extract the current number of outstanding POAMs currently in process (not completed). These POAMs may be linked by application, database, or infrastructure, so please ensure to capture all findings, including any audit action items. Place the Critical, High, and Moderate findings on the “Existing Findings” row by category. Next, collect any scan, audit, or other actionable findings that were created or discovered during this release’s project duration. Place the Critical, High, and Moderate findings on the “New Findings” row by category. Please be prepared to discuss any large number or existing findings, increase from new findings, or significant/Critical outstanding findings.

As of publication of the PRR Process Description 16.0 on July 29, 2016, FSA’s guidance on new vulnerability management tools is evolving (i.e. the CSAM implementation at FSA). An updated PRR Process Document and slide template are expected once more information is available on implementation of new tools.

PRR Template Version: 16.0

# Details of Security Vulnerability Findings

## Resolution of New Scan Findings

ID	Threat Level (Identified by Scan Tools – Crit/High/Mod)	Compensating Control Effectiveness (H/M/L)	Residual Risk Level**	Description of Finding	Affected System and Responsible ISSO	Mitigation Strategy: Corrective Action Plan (CAP) or Accepted Risk (AR)	Scan Type I=Infrastructure /OS A=Application D=Database

\*\* Residual Risk Level may be the same or lower than the initial threat level identified by Scan Tools due to compensating controls being in place.

26



PROUD SPONSOR of the AMERICAN MIND™

**Guidance for Slide 26:**

This slide provides the details on new findings from the vulnerability scans and other release activities. If a finding does not have an existing CAP or AR, it must be entered in FSA’s vulnerability management tools and an ID number obtained prior to the PRR.

## Operations and Maintenance

- Operations and Maintenance support for [System Name] is provided by [Contractor Name, FSA TO Application Support Team, etc.]
- The contract covering O&M support for this system is [contract name and number]
- [System Name] requires [number] of full time equivalents (FTEs) to support the system. [Note: This bullet is required for FSA In-House Development, but should be omitted for already-contracted O&M activities]
- The System Owner validates that the Configuration Management Plan for the system has been followed for this release and that appropriate configuration management practices are in place for the system.
- The System Owner has reviewed the backup schedule that is on file with the infrastructure provider (data center) and validated that appropriate backups are scheduled to occur.
- The System Owner validates that Capacity Planning activities have occurred or are scheduled for the system.

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 provides the details on the plan for operating and maintaining the system. Even if the PRR is for an update release to an existing system, this slide should be completed to show that the team is able to support continued operations. If there are operations and maintenance risks, such as a lack of support staff, that risk should be identified on this Open Risk slide. This slide revalidates system owner awareness/responsibilities for configuration management, backup, and capacity planning activities.

## 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]

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 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.

## LMM Tailoring and Technical Stage Gate Completion

Tailoring Plan / Technical Stage Gate (TSG)	Completed (Yes/No)	Date Completed / Approved	Comments
LMM Tailoring Plan	[Yes/No]	[Date]	[Provide the name of the LMM Tailoring plan and status comments. This plan describes the approach for the LMM Stage Gates and LMM Documentation Artifacts.]
Requirements Review (TSG3)	[Yes/No]	[Date]	[Describe the approach used to review the requirements for this release and to ensure that sound requirements management practices are in place for the system.]
Preliminary Design Review (TSG1A)	[Yes/No]	[Date]	[If stage gate was completed, please indicate the date that the design was reviewed by the Engineering Review Board (ERB). If stage gate not conducted according to LMM Processes, please explain what was done to meet the stage gate intent.]
Detailed Design Review (TSG1B)	[Yes/No]	[Date]	[If stage gate was completed, please indicate the date that the design was reviewed by the Engineering Review Board (ERB). If stage gate not conducted according to LMM Processes, please explain what was done to meet the stage gate intent.]
Test Readiness Review (TRR) – System Test (TSG2)	[Yes/No]	[Date]	[If stage gate was completed, please indicate the sign-off document(s) that can be provided. If stage gate not conducted according to LMM Processes, please explain what was done to meet the stage gate intent. For TSG2, there should be a completed and signed TRR checklist following the format in FSA’s Enterprise Test Management Standards.]
Test Readiness Review (TRR) – User Acceptance Test (TSG2)	[Yes/No]	[Date]	[If stage gate was completed, please indicate the sign-off document(s) that can be provided. If stage gate not conducted according to LMM Process, please explain what was done to meet the stage gate intent. For TSG2, there should be a completed and signed TRR checklist following the format in FSA’s Enterprise Test Management Standards.]
Production Readiness Review (PRR) (TSG4)	Yes	[Date]	The final signed version of this PRR Presentation documents the completion of TSG4.
Retirement Review (TSG5)	No	No system being retired.	This stage gate was not completed because this release does not retire a system. [Generally PRRs will not retire a system, adjust this text if necessary]

### Guidance for Slide 29:

This slide addresses the completion status of the LMM Tailoring Plan and of each of the LMM Technical Stage Gates. If the IPT has ensured a technical stage gate was completed following FSA’s documented LMM Technical Stage Gate Processes, then the Completed column should be marked as “Yes”. If the team has not followed the FSA documented LMM Technical Stage Gate process for a stage gate, then the Completed column should be marked as “No”. Please keep in mind that the LMM Stage Gates for requirements, design, and production readiness require reviews that are independent of the project team, so a project team review of the requirements or design document without consulting the Stage Gate Owners should be listed as “No.”

The IPT is strongly encouraged to review the stage gate criteria available on the LMM SharePoint site and to consult with the relevant stage gate owners regarding stage gates as the effort progresses and scope or implementation plans change. Such changes may require an update to the LMM Tailoring Plan. **The IPT should verify that this slide is in agreement with the LMM Technical Stage Gate information that is provided on their Release Request** – either the slide of the Release Request may need to be updated based on the actual reviews that were conducted.

Due to incomplete guidance on the Requirements Stage Gate (as of publication of this PRR Process Description), the requirements stage gate may be listed as a “Yes” response for releases that go through the Business Operations, FMS, and/or VDC Change Control Board Processes which the FSA Enterprise Quality Assurance Team has reviewed to validate that these processes are ensuring the correctness of individual requirements. Once guidance on the Requirements Stage Gate process has been published, this PRR guidance will be changed accordingly.

# System Documentation

[most recent version and update date should be identified in the table below, but updates are only needed on condition changes, not necessarily with each release]

Ent. WBS Code	Document	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 document, indicate the name of that document)
3.2.3	System of Records Notice (SORN)	[fill in document status from choices above]	[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]
3.9	Data Retention Schedule	[document status]	[version #]	[date]	[comments]
4.2	Requirements Management Plan	[document status]	[version #]	[date]	[comments]
5.1	Configuration Management Plan	[document status]	[version #]	[date]	[comments]
5.3	Detailed Design Document	[document status]	[version #]	[date]	[comments]
7.3	Operations and Maintenance Plan	[document status]	[version #]	[date]	[comments]
7.2	Training Plan	[document status]	[version #]	[date]	[comments]
**	OMB Information Collection Clearance (approval)	[document status]	[version #]	[date]	[comments]

### Guidance for Slides 30:

This slide addresses documents that are managed to support the information system. These documents may or may not need to be updated for a release and need to be evaluated on a case-by-case basis. For releases (projects) that have completed an LMM Tailoring Plan, the updates should correspond to the LMM Tailoring Plan. **The current version number and date of the document should always be reported** regardless of the update status of the document in relation to the release (this is done to show FSA Management that the document set for the information system is being appropriately maintained).

The document status options are explained below:

- Created Document – The document was created as part of the work within this release.
- Updated Existing Document – An existing document was updated as part of the work within this release.
- Part of Another Document – If the release used a single document to cover several document artifacts or if the document covering a particular item has a different scope than the item listed, this option should be used.
- No Update Needed – A relevant document exists and the IPT has reviewed the document and determined that the scope of the release or change does not necessitate updating the document.
- Not applicable to this release – This option should be used only of a document that does not apply in any form. This option should not be used for documents that cover the release, but apply at the system level.

# Release Documentation

[Documentation that should be new/changed/updated with each release]

Ent. WBS Code	Document	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 document, indicate the name of that document)
4.5	Detailed Requirements Document	[fill in document status from choices above]	[version #]	[date]	[comments]
4.6	Requirements Traceability Matrix	[document status]	[version #]	[date]	[comments]
4.7	Data Migration Plan	[document status] [If no data migration, list as "Not applicable to this release"]	[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]
6.3.3	Defect Management Report	[document status]	[version #]	[date]	[comments]
7.1.1	Implementation Plan	[document status]	[version #]	[date]	[comments]

## Guidance for Slides 31:

This slide addresses documents that are created as part of the release cycle (SDLC). These documents are created specifically for this release and relate specifically to the requirements for the release. For releases (projects) that have completed an LMM Tailoring Plan, the updates should correspond to the LMM Tailoring Plan. **The current version number and date of the document should always be reported** regardless of the update status of the document in relation to the release (this is done to show FSA Management that the document set for the information system is being appropriately maintained).

The document status options are explained below:

- Created Document – The document was created as part of the work within this release.
- Updated Existing Document – An existing document was updated as part of the work within this release.
- Part of Another Document – If the release used a single document to cover several document artifacts or if the document covering a particular item has a different scope than the item listed, this option should be used.
- No Update Needed – A relevant document exists and the IPT has reviewed the document and determined that the scope of the release or change does not necessitate updating the document.
- Not applicable to this release – This option should be used only of a document that does not apply in any form. This option should not be used for documents that cover the release, but apply at the system level.

## 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].
- The [role – project manager, system owner, system technical lead, etc] will be responsible for collecting the lessons learned and entering the lessons in the database.

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

32

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

PROUD SPONSOR of  
the AMERICAN MIND™

### Guidance for Slide 32:

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.

33

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

PROUD SPONSOR of  
the AMERICAN MIND™

### Guidance for Slide 33:

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.

## Support Contractor Sign-off

[Support Contractor Company Name] confirms that the information included in this PRR for **[System / Release Name and Version]** that is scheduled for implementation on **[implementation date]** is correct and accurate to the best of our knowledge. We confirm that testing and validation activities appropriate to the release have been completed. Further, [Support Contractor Company Name] confirms that all risks that we are aware of have been disclosed to the government in this PRR.

\_\_\_\_\_  
[Name]  
*Program Executive*

\_\_\_\_\_  
[Name]  
Project Manager

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 is the first of three sign-off pages for the PRR. Signatures from the support contractor management resources are required to ensure that the support contractor has disclosed all risks and validates that the information in the PRR is correct and accurate.

# 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]  
*Information Owner (Business Owner)*

\_\_\_\_\_  
Slawko Semaszczuk or designee  
*Virtual Data Center*

\_\_\_\_\_  
Linda Wilbanks or designee  
*FSA Chief Information Security Officer*

[Note: For releases outside of the VDC, the VDC sign-off is still is required to support coordination of system support and interfaces across the FSA organization.]

### Guidance for Slide 35:

This slide is the second of three sign-off pages for the PRR. Signatures from the project manager, system technical lead; test lead, ISSO, system owner, information 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 or designee  
*Enterprise Quality Assurance Program*

\_\_\_\_\_  
Leslie Willoughby, Wanda Broadus 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, number and complexity of system interfaces, release size, technology used by the release, implementation team maturity, and timing of the release implementation within FSA's business cycle.

Determination by Enterprise Quality Assurance Program:

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

\_\_\_\_\_  
Keith Wilson or designee  
*FSA Chief Information Officer*

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

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 is the third of three 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.

**Information Owner (Business Owner)** - The information 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, including related data, 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.

**Support Contractor Program Executive and Project Manager** - In addition to the Federal Officials listed above, the Support Contractor Program Executive and Project Manager supporting the release are required to sign-off on the PRR attesting to the government that information is accurate, appropriate testing has occurred, and that risks have been appropriately disclosed to the government.

## **Appendix A – Acronyms and Abbreviations**

## Appendix A - Acronyms and Abbreviations

ACS	Administrative Communications Systems
ATG	Assistive Technology Group
ATO	Authorization to Operate
ASI	Application Specific Information Document
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
CISO	Chief Information Security 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
CSAM	Cyber Security Assessment Management tool
ECCB	Enterprise Change Control Board
ECM	FSA Enterprise Change Management (Process and/or Tool)
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
ONR	Organizational Need Request
ORB	Organizational Review Board
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
RR	Release Request

RTO	Recovery Time Objective
SDR	Service Delivery Review
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SORN	System of Records Notice
SP	Special Publications
SRR	Security Readiness Review
TRB	Technical Review Board
TRR	Test Readiness Review
UAT	User Acceptance Testing
UI	User Interface
VDC	Virtual Data Center
VDD	Version Description Document
VSA	Vulnerability Scan Assessment

## **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	<p>Emergency -</p> <ul style="list-style-type: none"> <li>• Correct an application/system halt (abnormal termination) in the production environment</li> <li>• Correct a hazardous condition that may result in injury to personnel or damage to equipment</li> <li>• Effect a change in operational characteristics that, if not accomplished expeditiously, may seriously compromise security or business mission</li> </ul> <p>Urgent –</p> <ul style="list-style-type: none"> <li>• Effect a change that, if not accomplished, may compromise effectiveness, contractual commitments, life cycle costs, or business mission</li> <li>• Correct a condition that is affecting the system or system component that is critical</li> <li>• Effect a change in operational characteristics to implement regulatory requirements with stringent completion date requirements</li> </ul> <p>Routine –</p> <ul style="list-style-type: none"> <li>• Assigned when emergency or urgent implementation is not applicable, required, or justifiable</li> </ul>
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 Solution (Sandbox and Farm)	A Microsoft SharePoint Server 2010 <i>solution</i> is a deployable, reusable package that can contain features, site definitions, and

Term	Definition
Deployments)	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 <i>sandbox</i> . 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 <i>sandboxed solutions</i> , cannot use certain computer and network resources, and cannot access content outside the site collection they are deployed in.
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	<p>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.</p> <p>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.</p> <p>Patch: a change to fix a deficiency in the controlled item with no new functionality added.</p>