

U.S. Department of Education Federal Student Aid



START HERE
GO FURTHER
FEDERAL STUDENT AID[®]

Production Readiness Review (PRR) Process Description

Version 10.0

Final

July 30, 2010

Document Version Control

Version	Date	Description
10.0	7/30/2010	<ul style="list-style-type: none"> Removed sign-off types (i.e. conditional, provisional, etc). Expanded timeline of events in the PRR process to add planning steps earlier in the project lifecycle and to accommodate an optional review of test data by CIO Enterprise Testing Group. Minor re-organization of order and titles of information presented in PRR slides. Re-organized and updated PRR Checklist (Appendix C and D) to improve usability. Updates to appendices to support changes.
9.0	7/31/2009	<ul style="list-style-type: none"> Added LCM Framework reference (Section 1). Changes to sign-off for large-scale releases (Section 6). Added System Test Lead, FSA Computer Security Officer, and Responsible ELT Member descriptions to Sign-off requirements (Section 6). Clarifications to PRR Process steps, including better identification of the role of the QA Team (Section 4). Reformatted PRR Summary Checklist to portrait layout instead of landscape and removed risk mitigation columns (Appendix C). Reformatted PRR Summary Checklist Definitions to portrait layout instead of landscape and removed risk mitigation columns (Appendix D). Updated sample sign-off memo (Appendix E) Minor editorial changes for grammar, spelling, formatting, etc (entire document).
8.1	01/30/2009	<ul style="list-style-type: none"> Modified Applicability section to address concerns related conducting PRRs on infrastructure and toolset changes. Clarified the sign-off authorities for the CIO signature. Added Checklist items to cover re-validation of disaster recovery objectives (RTO and RPO) and vulnerability scans. Minor clarifications in PRR checklist definitions.
8.0	7/30/2008	<p>Major Document Revision includes the following:</p> <ul style="list-style-type: none"> Major Checklist updates to reflect stakeholder discussions New information regarding rationale for holding PRRs New diagram depicting the role of the PRR in the context of other related activities Addition of PRR presentation slides Updated signoff role descriptions Updates to signature page Updated terminology based on VDC Configuration Management Database (CMDB) Data Dictionary, ECOM, and Security documents. Major formatting and editorial changes to conform to the Federal Student Aid Document Template
1.0 - 7.0	6/19/2007	For previous revision history of Versions 1.0-7.0, see Version 7.0

TABLE OF CONTENTS

SECTION 1. LEGISLATIVE BACKGROUND.....	1
SECTION 2. PURPOSE.....	2
SECTION 3. APPLICABILITY	3
SECTION 4. PRR PROCESS STEPS.....	4
SECTION 5. PRR PRESENTATION OUTLINE	9
SECTION 6. SIGN-OFF	12
SECTION 7. SIGN-OFF RESPONSIBILITIES	15
SECTION 8. DELIVERABLES.....	17
APPENDIX A - ACRONYMS AND ABBREVIATIONS.....	18
APPENDIX B - GLOSSARY	21
APPENDIX C - SUMMARY CHECKLIST	23
APPENDIX D - CHECKLIST DEFINITIONS.....	31
APPENDIX E - SAMPLE PRR SIGN-OFF MEMO.....	43
APPENDIX F - REFERENCES	45
APPENDIX G – PRR SLIDE TEMPLATE.....	47

SECTION 1. LEGISLATIVE BACKGROUND

The Production Readiness Review (PRR) Process has been put in place by Federal Student Aid to reduce the likelihood of new releases causing unintended adverse impact to FSA's business or end-users. This process also supports the responsibilities of Federal Student Aid's 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.

In addition, the PRR is intended to support the requirements of the third Stage Gate Review (between the Construction & Validation and Implementation Stages), as described in the Department of Education's directive on the Lifecycle Management Framework (OCIO: 1-106, dated 12/02/2005).

SECTION 2. PURPOSE

The purpose of the PRR is to establish a common process that defines the activities and the roles of all groups supporting the government's decision to implement a new information system or a new release of an existing system. The PRR serves as the final, formal, and documented decision point before a new system or a significant release of an existing system enters Federal Student Aid's production environment and is exposed to end-users.

Completion of a PRR accomplishes the following:

- Demonstrates to Federal Student Aid's senior management the readiness of the system to enter production.
- Reviews the testing approach, participation, and test results to ensure that the system has been adequately tested and is ready for use by end-users.
- Discloses areas of risk associated with the system moving into production and the associated risk mitigation strategies. This ensures that Federal Student Aid Management is aware of all risks associated with a release and has accepted the risk of implementing the system. For systems where users are Trading Partners, Students, Parents, or Borrowers, completion of a PRR acknowledges that Federal Student Aid management has accepted the risks associated with public exposure of the system.
- Reviews Lessons Learned and Process Improvements
- Documents formal authorization to move the system into production as indicated by completion of a PRR Sign-Off Memorandum (Appendix E).

SECTION 3. APPLICABILITY

The PRR Process applies to initial releases of applications entering Federal Student Aid’s Data Center Production Environment. The PRR Process also applies to significant enhancements to existing applications. An application consists of business logic that directly impacts end-users (students, parents, schools, financial aid administrators, borrowers, lenders, guarantee agencies, government employees and contractors).

The PRR Process is not required for releases that are solely related to the deployment of infrastructure (e.g. changing a router). The PRR Process is also optional for emergency releases, operating system upgrades and patches (including midrange and mainframe operating system upgrades), upgrades and patches to commercial-off-the-shelf software (COTS) that do not impact end users, and build-out of tool sets within the operating environment.

While the PRR Process is optional for infrastructure and tool sets when they are initially deployed, these items are a critical component of supporting applications in the operating environment and must be taken into consideration when an application team performs a PRR.

<u>General Guide for PRR Applicability</u>	
Release Description	PRR Required or Optional
Applications (initial releases and significant enhancements) – Includes all business logic that impacts end users.	Required
Infrastructure – Includes all hardware and operating system components.	Optional
Significant COTS releases that impact end users	Required
COTS Upgrades and Patches that do not impact end users	Optional
COTS-based Tool Sets – Releases that deploy tool sets into the operating environment and do not impact end users.	Optional
Re-design of websites	Required
Minor content updates to websites	Optional

Federal Student Aid’s Chief Operating Officer (COO), Chief Information Officer (CIO), or the Virtual Data Center (VDC) Manager may request that a PRR be completed for any release. If the Application Owner disagrees with this request, the application may not enter the production environment until FSA’s CIO and other members of the leadership team have made a determination.

If project teams have questions related to the applicability of PRR to a particular release, those questions should be resolved at the weekly VDC Projects and Operations Meeting or by coordinating with the CIO Enterprise Quality Assurance Team.

SECTION 4. PRR PROCESS

PRR Process Steps

The PRR is a critical meeting that is the final decision point in the development process before implementation begins. The following diagram shows the PRR meeting in the context of other critical activities related to the implementation release schedule.

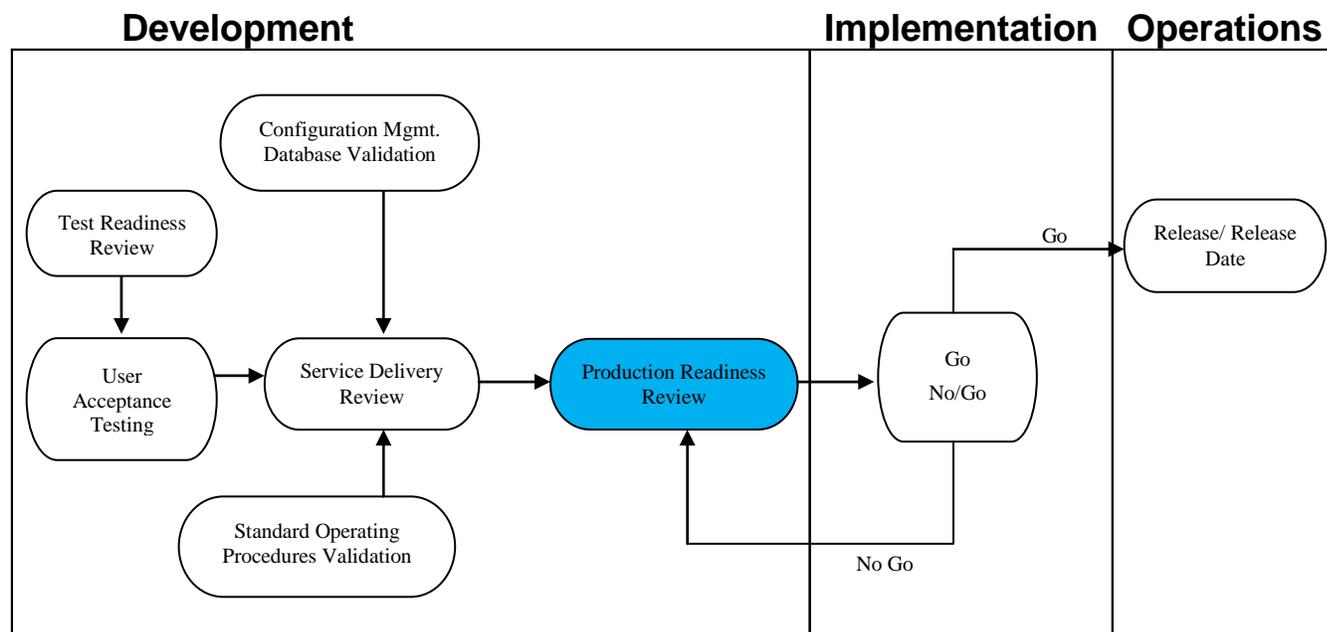


Figure 1, Role of PRR Process

The following table provides the process steps and timeline for the PRR Process. The Project Team developing a system release has primary 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 will be driven by project dependencies and other constraints. The steps in the table are explained in the descriptions below the table.

#	PRR Process Step	Timeframe (T = Production Date)	Timeframe Flexibility
1	PRR Checklist items incorporated in development lifecycle and project schedule and monitored throughout project	Project inception and monitored throughout project.	N/A
2	QA Team initial coordination with project team	T – 90 calendar days (or as soon as practical)	QA Team proactively monitors for PRR events. System teams should schedule a PRR with at least 30 business days notice.

3	Provide test schedule and plans to CIO Enterprise Testing Group. (Recommended Optional Activity – see description in text below this table)	During FSA review process prior to acceptance by the FSA business owner.	N/A – it is critical that this activity occur so that timely feedback on testing planning decisions can be provided early in the process.
4	Provide system test results to CIO Enterprise Testing Group (Recommended Optional Activity – see description in text below this table)	At completion of system test and before start of UAT	N/A – it is critical that this activity occur at this point so that timely feedback can be provided. Feedback will consist of recommendations for future process improvements.
5	System Team Operational Readiness Review (ORR)	Determined by Project Team, but should be conducted before Pre-PRR.	Determined by Project Team.
6	Pre-PRR with key enterprise stakeholders (Recommended Optional Activity)	T – 14 business days	Optional Activity, but strongly recommended prior to actual PRR.
7	Provide UAT results and Accessibility Testing (508 Compliance) results to CIO Enterprise Testing Group (Recommended Optional Activity – see description in text below this table)	T – 12 business days	N/A – it is critical that this activity occur at this point so that timely feedback can be provided.
8	Draft of PRR materials distributed	T – 12 business days	T-12 business days is preferred, T-10 business days is adequate.
9	Service Delivery Review (SDR) by Data Center Contractor. A review of the Configuration Management Database entries for the system is performed as part of the SDR.	If Applicable, SDR must be completed prior to PRR. Any outstanding issues from SDR must be reported at PRR.	If applicable, SDR must be completed prior to PRR.
10	PRR Presentation and Sign-Off	T – 5 business days	T – 5 business days is strongly recommended, in case corrective actions are needed prior to production.
11	Release Production Date	T	N/A

PRR Preparation (Steps 1 - 4)

During the initial planning of a system release, the items on the PRR Checklist (Appendix C) should be included in the project plan, project schedule, and any support contracts. It is the

responsibility of the Project Team within FSA that is managing the release to appropriately plan and coordinate these activities and deliverables.

As the release moves through its lifecycle, the status of PRR Checklist items should be monitored as part of the project schedule.

It is recommended that testing activities be coordinated with the CIO Enterprise Testing Group (see Appendix D for points of contact), as follows:

- Send test plans during FSA review process prior to acceptance by FSA.
- Send system test results at completion of system test and before start of User Acceptance Testing (UAT).
- UAT results T – 12 business days (at least 12 business days before the production implementation date).

The CIO Enterprise Testing Group will provide feedback on the test plans and results of testing and provide feedback for process improvement purposes in future releases. Since this feedback is for long term process improvement, it is not critical that the review be completed before moving forward with the release.

Once development and testing activities are complete, the Project Team prepares for a PRR by reviewing and finalizing documentation for system as well as executing activities to prepare for implementation of the release. The team also prepares a PRR briefing (slide presentation) and completes the PRR Checklist.

Collaboration (Steps 5-9)

The Project Team should collaborate with other areas of Federal Student Aid that support the system release to implement the following functions:

- Identify all external organizations and representatives who will participate in the PRR process, including the data center, other impacted systems (if any), security staff, the CIO Enterprise Testing Group, CIO Enterprise Quality Assurance (QA) Team, and others as appropriate.
- Coordinate with the Enterprise Operational Change Management (EOCM) process, as required, for all enterprise events. Enterprise events include changes that impact more than one system.
- Coordinate with the CIO Enterprise Testing Group to review test plans and test results for System Testing and User Acceptance Testing (UAT) and obtain feedback for testing process improvement. While not required, this is a strongly recommended optional activity that Enterprise Quality Assurance will ask about in reviewing PRR materials.
- Complete the PRR Checklist and identify any incomplete items that should be completed before the release moves to the production environment. There is a cost-benefit decision to completing each of the checklist items for a given release. The cost-benefit trade-off should be considered by the Project Team as part of the project planning and system

development process and any decision not to complete a checklist item should be explained at the PRR Presentation.

- Any open project risks and the associated risk mitigation strategies should be documented and the project team should make a determination to accept the risks, mitigate the risks, or delay the release.
- Discuss the PRR presentation outline with the Project Team, System Team, and CIO contacts prior to the formal presentation to address specific concerns that senior managers may have with the release.

Prior to the PRR, the Project Team should contact the CIO Enterprise Quality Assurance Team. The CIO Enterprise Quality Assurance Team will work with the project team to identify the appropriate participants in the PRR. This will involve the CIO Enterprise Quality Assurance Team gaining an understanding of the scope of the release so that the CIO Enterprise Quality Assurance Team can make a judgment as to overall enterprise impact of the release. Releases that have a significant impact to the FSA enterprise will need signatures from the CIO and the Operating Committee member responsible for the business process of the release entering production. The CIO Enterprise Quality Assurance Team is responsible for coordinating the appropriate CIO staff to attend the PRR for sign-off.

Ideally, the CIO Enterprise Quality Assurance Team will be notified of the release at least 90 days in advance of the PRR meeting and will be provided with a copy of the presentation slides and completed PRR Checklist at least 5-7 business days in advance of the PRR Presentation meeting. The CIO Enterprise Quality Assurance Team will coordinate distribution of PRR materials to the appropriate stakeholders in CIO. Detailed supporting documentation, including a completed PRR Checklist (Appendix C) and documentation of any incomplete items or open risks listed, should be reviewed by the CIO Enterprise Quality Assurance Team and other appropriate parties prior to the PRR.

To ensure that all documents are ready for the formal PRR and there are no outstanding issues that need to be resolved prior to the PRR, it is strongly recommended that the project team hold a "pre-PRR" with the system team, the Independent Verification & Validation (IV&V) contractor (if applicable), the security team (including both the application ISSO as well as CIO Security & Privacy), the CIO Enterprise Testing Group, the CIO Enterprise Quality Assurance Team, and teams associated with testing the system. The pre-PRR meeting should consist of reviewing the PRR Presentation and PRR Checklist based on the current status of the release. The focus should be on explaining the status of any open risk items.

The PRR Checklist is reviewed at both the Pre-PRR and PRR to verify that all that appropriate documentation has been created or updated for the release and that key activities have been completed. If a checklist item is not appropriate to the release, the system team should indicate "N/A" (not applicable) on the checklist. Appendix C of this document includes the PRR Checklist. Appendix D includes definitions, clarifications, and points of contact for each checklist item.

Presentation and Sign-Off (Steps 10-11)

A PRR meeting must be held to provide a forum for formal discussion and approval of the release moving to the production environment. The System Technical Lead or Project Team Lead is responsible for directing the preparation of the presentation and selecting the appropriate presenter(s). The presentation is delivered by the System Technical Lead or Project Team Lead. Contractor staff may provide support to the presentation, but may not sign-off on the PRR Memorandum. The presentation should not exceed one hour in length, including questions and answers. The presentation is an executive overview of the production readiness of the system release.

See Section 6 and Section 7 of this document for sign-off procedures and responsibilities.

SECTION 5. PRR PRESENTATION OUTLINE

The presentation outline may be customized to meet the needs and interests of the application owner and Federal Student Aid's CIO; however, all information included in the outline below must be covered, in some form, during the presentation. Additional information and issues may be included in the PRR presentation, as necessary.

I. Business Background

- Description of the major functions of the system
- Business benefits, improvements, and enhancements that are being introduced by this release.

II. Schedule

- Planned Development Schedule (Baseline)
- Actual Schedule
- Schedule information must specifically show the time that was allotted for testing activities.

III. Review of Open Risks

- Open risks associated with implementation of the release and mitigation strategies
- Outstanding Issues/Action Items
- Specific identification of known risks that are being accepted with the decision to implement the release

IV. Data Center Readiness

- CMDB Validation Complete
- Service Delivery Review (SDR) Status and Outstanding Issues
- Disaster Recovery Objectives
- Service Desk Notification
- Status of Implementation Change Request

V. Testing Summary

- High Level Test Summary. This includes the types of tests conducted (Integration, System, Inter-system Testing, User Acceptance Testing, 508 Accessibility Testing, Performance and Capacity Testing, and Security) including high level issues found by each phase of testing that is performed for the particular project.
- Defect Report by Testing Phase. This slide includes total number of defects identified by criticality (Urgent, High, Medium and Low) within each type of testing and categorized by the statuses of Open, Closed, Deferred and Enhancements.
- Describe any urgent and high severity defects that were found during system testing and during user acceptance testing.

VI. Information System Security and Privacy

- Impact of the release to the security posture of the system
- Revalidate security categorization for the system

VII. End User Support Readiness

- Readiness of Help Desk / Call Center

VIII. Communication to End Users

- Address the communications (content and timing) that will be sent to end users to notify them of the new features contained in the release and of any down time (ie. An outage message will be posted on the website to notify users that the side is down for maintenance).

IX. Independent Verification & Validation (IV&V), if applicable

- Summary of approach, activities, and results.
- IV&V Recommendation (Go, Go with Reservations (list reservations), No Go); IV&V's recommendation is based on all requirements being implemented and tested and there being no critical defects. IV&V will notify the Project Team and the CIO Enterprise Quality Assurance Team prior to the PRR if a recommendation is conditional or a "No Go."
- The IV&V section only applies to releases that have an IV&V Team supporting the release. If there is no IV&V Team supporting the release, this section should be marked as "Not Applicable" or may be removed.

X. Lessons Learned

- Describe key lessons learned to this point in the project.

- State how lessons learned will be captured and maintained.

XI. Meeting Closure

- Completion of formal sign-off memorandum
- Delivery of sign-off memorandum and supporting documentation to CIO QA Team (may be completed after meeting)

SECTION 6. SIGN-OFF

The primary output of the PRR Meeting is a memorandum that formally authorizes a system or release to move into the production environment. A sample sign-off memorandum is presented in Appendix D. The sign-off memorandum may be tailored to the needs of the project, subject to the following conditions:

1. Only government employees may sign the memorandum (contractors may not sign). A PRR represents the government's decision to implement a release and the government's acceptance of risk associated with that implementation. It is suggested that government staff obtain a separate memorandum from contractors recommending Go or No/Go at a PRR, but the final decision to implement (or not to implement) a release must be made by government staff.
2. The following are the signatures required for sign-off:
 - System Test Lead
 - Information System Security Officer (ISSO)
 - System Technical Lead
 - System Owner (optional, depending on business area)
 - Application Owner
 - FSA's Chief Information Security Officer (CISO) (CIO)
 - Virtual Data Center Manager (CIO)
 - Enterprise Quality Assurance Program Manager (CIO)
 - CIO Management*
 - FSA's CIO*
 - Operating Committee Member responsible for the system/release*

In the event sign-off does not occur, concurrence should be reached on the action items, activities, or deliverables that must be completed. Once the action items are addressed, another PRR presentation is required and will be held prior to approval being given.

*The need for PRR Sign-off by CIO Management and FSA Senior Management is determined and by sign-off threshold for the release. The CIO Enterprise Quality Assurance Team will determine the sign-off threshold for each released, based on the following criteria:

Sign-off Threshold	Release Description	Sign-offs Required
High	<p>Initial releases of major applications and system integration projects, or;</p> <p>Significant updates that have a major impact on the way that FSA does business and/or affect a large number of external customers.</p>	<ul style="list-style-type: none"> • System Test Lead • Information System Security Officer (ISSO) • System Technical Lead • System Owner (optional, depending on business unit responsibilities) • Application Owner • FSA’s Chief Information Security Officer (CISO) (CIO) • Virtual Data Center Manager (CIO) • Enterprise Quality Assurance Program Manager (CIO) • CIO Management • FSA’s CIO • Operating Committee Member responsible for the system/release
Moderate	<p>Routine updates to major applications, initial releases of non-major applications, and large-scale annual releases.</p>	<ul style="list-style-type: none"> • System Test Lead • Information System Security Officer (ISSO) • System Technical Lead • System Owner (optional, depending on business unit responsibilities) • Application Owner • FSA’s Chief Information Security Officer (CISO) (CIO) • Virtual Data Center Manager (CIO) • Enterprise Quality Assurance Program Manager (CIO) • CIO Management
Low	<p>Mid-size (or smaller) changes to application business logic that are routine in nature, releases where the only end-users are government employees or contractors, and releases that pose a low overall risk to Federal Student Aid’s core business.</p>	<ul style="list-style-type: none"> • System Test Lead • Information System Security Officer (ISSO) • System Technical Lead • System Owner (optional, depending on business unit responsibilities) • Application Owner • FSA’s Chief Information Security Officer (CISO) (CIO) • Virtual Data Center Manager (CIO) • Enterprise Quality Assurance Program Manager (CIO)

SECTION 7. SIGN-OFF RESPONSIBILITIES

System Test Lead - The System 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 end-users.

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

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

System Owner - The system owner's signature certifies that all reasonable due diligence has been exercised to assure system stability/operability, that known risks have been identified/described in the presentation, and that an appropriate business benefit will be derived by the implementation of the system.

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

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.

Enterprise Quality Assurance Program Manager (CIO) - 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.

FSA's Chief Information Security Officer (CIO) – The CISO's signature certifies that the system has received authority to operate and has completed all security and privacy documentation that is needed prior to the release entering production.

Virtual Data Center Manager (CIO) - The Government 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.

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

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.

SECTION 8. DELIVERABLES

The following deliverables should be distributed to the System Technical Lead (originals), the Project Manager (if different than the technical lead), and the CIO Enterprise Quality Assurance Team (POC: Trey Wiesenburg).

- Completed PRR Sign-off Memorandum
- PRR Presentation
- PRR Checklist
- Supporting Documentation

Hard copies of all the materials should be available at the PRR Presentation. As described in Section 4, draft copies (electronic) of the PRR Presentation and Checklist should be sent out ahead of the meeting so that there is sufficient time for all participants to review the information. The final versions of all the deliverables should be provided electronically to meeting participants immediately ahead of the meeting. Following the formal PRR meeting, the documentation (with any revisions from the meeting) may be delivered to the CIO Enterprise Quality Assurance Team in either electronic or hard copy; however electronic (PDF) is preferred.

Appendix A – Acronyms and Abbreviations

Appendix A - Acronyms and Abbreviations

ACS	Administrative Communications Systems
ATG	Assistive Technology Group
ATO	Authorization to Operate
C&A	Certification & Accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
COO	Chief Operating Officer
COR	Contracting Officer Representative
COTS	Commercial-off-the-Shelf
CISO	Chief Information Security Officer
ED	Department of Education
EIT	Electronic and Information Technology
EOCM	Enterprise Operations Change Management
EQA	Enterprise Quality Assurance
FIPS	Federal Information Processing Standard
G.A.	Guarantee Agency
GAO	General Accounting Office
GPRA	Government Performance and Results Act of 1993
IATO	Interim Approval to Operate
IEEE	Institute of Electrical and Electronics Engineers
IPC	Investment Planning Council
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
NIST	National Institute of Standards and Technology

OCIO	Office of the Chief Information Officer
OMB	Office of Management & Budget
ORR	Operational Readiness Review
PIR	Post-Implementation Review
POC	Point of Contact
PRR	Production Readiness Review
QA	Quality Assurance
RACI	Responsibility, Accountability, Communication, Informed
SDR	Service Delivery Review
SLA	Service Level Agreement
SP	Special Publications
SRR	Security Readiness Review
TRR	Test Readiness Review
UAT	User Acceptance Testing
VDC	Virtual Data Center

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). (Definition Source: Created by the group in a meeting)
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 (SA), WebSphere Application Cluster Server, Oracle DBMS Clusters). (Definition Source: Created by the group in a meeting)
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)
Operational Readiness Review (ORR)	Review performed by the project team (both federal staff and contractors) that is directly responsible for the development of a release of an information system or system component.
Production Readiness Review (PRR)	Review performed by the Federal Student Aid enterprise to ensure that a release of an information system or system component will perform as intend in the production environment and that the release meets 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 this is produced through a software development process or commercial-off-the-shelf (COTS) implementation. (Definition Source: Created by the group in a meeting)
Independent Verification and Validation (IV&V)	IV&V is a process used to assure that the products of a system development activity meet the requirements of that activity and the delivered system satisfies the intended use and user needs. Large scale system development projects in the government often use a team that is independent of the project to review many aspects of the project.

Appendix C – Summary Checklist

PRR Checklist for [System/Release Name]

Checklist Guidance:

This checklist includes the items that are examined as part of Production Readiness Review. The checklist may be tailored to the particular needs of each release. Please consult with the CIO Enterprise Quality Assurance Team if extensive tailoring is needed to support your release. A final version of the checklist may indicate that a gap exists (e.g., user training was not completed); in such cases, the managers attending the PRR will make a decision about signing off on the PRR with a gap present. A checklist item that is applicable, but incomplete, indicates a risk that needs to be addressed at the PRR. Definitions, roles, and responsibilities of the items on this checklist are included in Appendix D of this PRR Process Description (this document).

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Status of document for this release: - document created - document updated - no update needed - document not applicable to this release	Document Version Number	Date of last Document Update	Comments
1	Project Concept Document and/or OMB 300				
2	Initiative Vision				
3	High Level Requirements				
4	Project Charter				
5	Project Management Plan (schedule, requirements, quality, risk, and performance)				
6	Privacy Threshold Analysis / Privacy Impact Assessment				
7	Inventory Worksheet				
8	Implementation / Transition Management Plan				
9	User Interface (UI) Specification				
10	Detailed Requirements				

	Document				
11	IT Contingency Plan				
12	Master Test Plan (includes System Test Plan and User Acceptance Test Plan)				
13	System Security Plan				
14	Configuration Management Plan				
15	Preliminary Design Document				
16	Detailed Design Document				
17	Security Risk Assessment & Mitigation Plan				
18	Operations & Maintenance Plan				
19	Requirements Traceability Matrix				
20	Test Suites (includes cases and scripts)				
21	Iteration Status Report				
22	Solution Source Code and Deployable Packages	Source code complete and ready to deploy to production. [this statement must be true to begin a PRR]	Software version number of this release:	Actual or Anticipated Date of final build for this release:	[Note: this line is addressing software build information. See your configuration manager to obtain this information]
23	System Test Summary Report				
24	User Acceptance Test Summary Report				
25	Production Readiness Review (PRR) Report (Report consists of Slide Presentation, PRR Checklist, and Sign-off Memo)				[This checklist]
26	Training Plan				
27	Solution User Manual				
28	Version Description Document				
29	Security C&A and Post-Implementation Evaluation				

30	System Retirement Plan	[likely status is “document not applicable to this release;” however, if this release replaces or retires another system, then the system retirement plan for that other system should be addressed in this item]			
31	System Disposal Plan	[likely status is “document not applicable to this release;” however, if this release replaces or retires another system, then the system disposal plan for that other system should be addressed in this item]			

Section 2: Data Center Readiness			
This section of the PRR Checklist reviews the activities needed to coordinate readiness of the data center to support the release moving in to the production environment.			
#	Activity / Question	Status / Response	Comments / Documentation Reference
32	Identify the data center(s) where the release will be implemented.	[VDC, TSYS, Vangent, etc. If more than one, please list all locations being impacted by the release]	[Include city and state location of data center]
33	Operational Roles and Responsibilities defined	[Yes / No]	[Identify document where the roles and responsibilities for operational activities are defined]
34	Configuration Management Database (CMDB) updated, if necessary.	[Yes / No]	[Indicate date of last CMDB review]
35	VDC Service Request (Request for VDC Services Form) submitted	[Yes / No / NA]	[Indicate Capture Control Number and date if it was submitted, reason for not submitting, or reason for not applicable]
36	Change Request Submitted for Production Migration	[Yes / No / NA]	[Indicate Change Request Number and date submitted]
37	VDC Service Delivery Review (SDR) Completed	[Yes / No / NA]	[Indicate date that the SDR was completed and any outstanding issues from the SDR that need to be resolved prior to production implementation. Outstanding issues should be included in PRR Presentation slides as well.]
38	Revalidate Disaster Recovery Objectives based on the functionality changes being introduced by this release.	[System is Mission Important , RTO: 48 hours, RPO: 24 hours. or Mission Supportive , RTO: 72 hours,	[Note: If the system is located at the VDC, this information should match the information included in the VDC Continuity of Services Plan. If this release changes the Disaster Recovery needs of the system, then the VDC Disaster Recovery Team should be notified.]

		RPO: 48 hours.]	
--	--	-----------------	--

Section 3: Testing			
This section of the PRR Checklist reviews the testing activities that were conducted for this release.			
#	Activity / Question	Status / Response	Comments / Documentation Reference
39	Was a test readiness review performed prior to the start of System Testing?	[Yes / No / NA]	[Date of Test Readiness Review]
40	Was the organization that performed system testing part of the development organization or independent of the development organization?	[Developer conducted system testing / Independent organization conducted system testing / NA]	[Note: It is desirable to have an independent organization perform system testing, however system testing is performed by the developer in most cases at FSA.]
41	Have all defects identified in system testing been resolved?	[Yes / No / NA]	[Include any open / unresolved defects in PRR slide presentation]
42	Have the results of System Testing been submitted to the CIO Enterprise Testing Group for review? (Recommended Optional Activity)	[Yes / No / NA]	[Indicate submission date]
43	Was performance testing conducted for this release?	[Yes / No / NA]	[Indicate start and end date of performance testing activities]
44	What were the performance targets established for the application?	[Describe performance targets, such as estimated number of concurrent users, estimated submissions per hour, etc]	
45	Were the performance targets met during performance testing?	[Report on actual performance test results]	
46	If performance testing was conducted, was the application stress-tested and what was the maximum load?	[Application was stress tested for this release / application was not stress tested for this release]	[If application was stress tested, please indicate the maximum load that the application can accommodate (i.e. maximum number of concurrent users, maximum number of submissions, etc. If application was not stress tested, please explain reason for not performing this test]
47	Accessibility (508 compliance) testing performed for this release.	[Yes / No / NA]	[Indicate date of 508 test. If not performed, please explain why not.]
48	Did Accessibility (508 compliance) testing pass or fail?	[Passed / Failed / NA]	[If testing failed, please discuss in the PRR slide presentation.]
49	Was a test readiness review performed prior to the start	[Yes / No / NA]	[Date of Test Readiness Review]

	of User Acceptance Testing?		
50	Did FSA personnel (government employees) execute the user acceptance testing?	[Yes / No / NA]	[If FSA personnel did not execute user acceptance testing, please explain]
51	Have all defects identified in user acceptance testing been resolved?	[Yes / No / NA]	[Include any open / unresolved defects in PRR slide presentation]
52	Have the results of User Acceptance Testing been submitted to the CIO Enterprise Testing Group for review? (Recommended Optional Activity)	[Yes / No / NA]	[Please indicate submission date]

Section 4: Information System Security and Privacy			
This section of the PRR Checklist reviews the status of information system security and privacy for the application and the impact of this release on information system security and privacy.			
#	Activity / Question	Status / Response	Comments / Documentation Reference
53	Application Owner Identified	Name:	
54	Information System Security Officer (ISSO) Identified	Name:	
55	Does this system currently store or process Personally Identifiable Information (PII)?	[Yes / No]	
56	Will implementation of this release cause the system to store or process Personally Identifiable Information (PII)?	[Yes / No]	
57	Has the ISSO reviewed the impact of this release on the security posture of the system?	[Yes / No]	[Indicate the date that the review was completed]
58	Revalidated FIPS 199 Security Categorization based on this release.	[High / Moderate / Low]	
59	Is a new security authorization (formerly C&A) required as part of this release?	[Yes / No]	
60	Is an Authority to Operate (ATO) in place for the system?	[Yes / No / NA]	[Indicate date that ATO was signed]
61	Is a human and machine readable privacy policy included on public-facing websites?	[Yes / No / NA]	
62	Has a privacy threshold analysis been completed?	[Yes / No / NA]	

63	If required, was a Privacy Impact Assessment Completed?	[Yes / No / NA]	[Note: the privacy threshold analysis will determine if a Privacy Impact Assessment is required]
64	If required, was a system of record review completed?	[Yes / No / NA]	
65	Was an initial or updated System of Records Notice (SORN) published for this release?	[Yes / No / NA]	[Indicate date of SORN publication and Federal Register Reference]
66	If Personally Identifiable Information (PII) is used to uniquely identify individuals, have alternatives been considered?	[Yes / No / NA]	[Indicate date when alternatives were last considered and the outcome.]
67	Have vulnerability scans of stage or test environment been conducted for this release? Note: Some applications do not have a stage environment or do not update their stage environment until immediately before production. In those cases, the test environment is scanned instead of the stage environment.	[Yes / No / NA]	Date scans conducted:
68	Have all scan findings been addressed for development, test, and stage environments?	[Yes / No / NA]	[Describe any findings that are still open]
69	Have vulnerability scans for the production environment been scheduled soon after the implementation of this release?	[Yes / No / NA]	Date scans scheduled:

Section 5: Support Readiness			
This section of the PRR Checklist reviews the readiness of support services that are in place to support users.			
#	Activity / Question	Status / Response	Comments / Documentation Reference
70	Has the data center service desk been notified of the release?	[Yes / No / NA]	
71	Have data center operating procedures been updated based on this release?	[Yes / No / NA]	
72	Has the help desk (or call center) that supports end users been notified of this release?	[Yes / No / NA]	
73	Has the help desk (or call center) been trained on the	[Yes / No / NA]	Date of Training:

	changes being implemented by this release?		
74	Have help desk (or call center) scripts been updated based on this release?	[Yes / No / NA]	

Section 6: Communication to End Users			
This section of the PRR Checklist reviews the communication of this release to end users.			
#	Activity / Question	Status / Response	Comments / Documentation Reference
75	If an extended outage window is needed to implement this release, will communication be sent to end users?	[Yes / No / NA]	Date end users were / will be notified:
76	If a website is involved, will a message be posted during the outage?	[Yes / No / NA]	

Appendix D – Checklist Definitions, Roles and Responsibilities by Checklist Item

Appendix D - Checklist Definitions, Roles and Responsibilities by Checklist Item

The teams that are generally involved in the Production Readiness Review Process include:

Team	General Responsibility in PRR Process	Point(s) of Contact
Project Team	Team of individuals (both federal and contractors) that are responsible for developing a system release.	Varies depending on the system/release.
System Team	Team of individuals that is responsible for the day-to-day operations of information system in direct support of FSA's business (generally this includes system staff in a FSA business unit). In most cases this team is the same as the project team. In some cases there will be a project team creating a release that hands off that release to the System Team to perform O&M activities.	Varies depending on the system/release.
CIO Enterprise Quality Assurance Team	Responsible for the enterprise PRR Process, ensuring that releases follow the PRR standards, and reviews the contents of PRR materials for risk related to implementation of the system.	Primary: Trey Wiesenburg Secondary: Mike Rockis
CIO Enterprise Testing Group	Group that creates and maintains FSA's enterprise standards for testing of information systems. This group also performs reviews of test artifacts to support continuous process improvement of testing activities throughout FSA.	Primary: Karen Edwards
IV&V Team	Provides recommendation at PRR based on their review of the release under development.	Primary: Trey Wiesenburg Secondary: Mike Rockis

The following checklist definitions and points of contact are provided to support preparation activities. If additional clarification on how to report an item in the checklist is needed, please see the CIO Enterprise Quality Assurance Team.

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
1	Project Concept Document and/or	The Project Concept Document explains the	Application Owner /	Enterprise Performance	Carole Kuriatnikova

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
	OMB 300	<p>scope and purpose of a funding request, supported by alternatives analysis and financial information.</p> <p>The Exhibit 300 (required by OMB) justifies the business case for an investment, to fill the gap in the organization's ability to meet the strategic goals and objectives with the least life-cycle costs of all the various possible solutions and provide risk adjusted cost and schedule goals and measurable performance benefits.</p>	System Manager	Management Services (EPMS) / Project Management Office (PMO)	
2	Initiative Vision	The Initiative Vision Document describes in detail Federal Student Aid's stakeholder needs and business problems to be addressed by the features or capabilities of the new Initiative, high-level business processes, and system context of the envisioned solution.	Application Owner / System Manager / Requirements Team	Not yet established.	Not yet established.
3	High Level Requirements	The High Level Requirements Document captures high level functional and non-functional requirements in the form of declarative statements.	Application Owner / System Manager / Requirements Team	Not yet established.	Not yet established.
4	Project Charter	The Project Charter identifies the project by specifying a need or problem to be solved. It outlines the project and covers its scope, project objectives, project roles and responsibilities, project approach and project deliverables. This document will be	Application Owner / System Manager / Requirements Team	Enterprise Performance Management Services (EPMS) / Project Management Office (PMO)	Carole Kuriatnikova

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
		developed by Federal Student Aid.			
5	Project Management Plan (schedule, requirements, quality, risk, and performance)	The Project Management Plan describes how contractors should address planning and scoping; governance; organizational change management; stakeholder management; requirements management; communications management; risk management; issues management; resource management; quality management; performance management; status reporting; evaluation; and, closure of the project.	Application Owner / System Manager	Enterprise Performance Management Services (EPMS) / Project Management Office (PMO)	Carole Kuriatnikova
6	Privacy Threshold Analysis / Privacy Impact Assessment	The Privacy Impact Assessment is used to identify if a system contains privacy information and lets the public know what information is collected and how it is secured. Information collected may include Social Security Numbers, PINs, Addresses, Dates of Birth, etc.	Information System Security Officer (ISSO)	CIO / Security and Privacy Team	Bob Ingwalson
7	Inventory Worksheet	The Inventory Worksheet is used to classify a system as either a general support system (GSS) or a major application (MA), identify data sensitivities, and to ensure that the system has the appropriate level of security.	Information System Security Officer (ISSO)	CIO / Security and Privacy Team	Bob Ingwalson
8	Implementation / Transition Management Plan	The Implementation Plan describes the planned procedures for releasing	Application Owner / System	Not yet established.	Not yet established.

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
		<p>the new system or system module to production. It lists deployment goals; critical success factors; deployment tasks; resources, and tools; task and resource dependencies; task responsibilities and timelines for completion; and significant risks and contingency plans.</p> <p>The Transition Management Plan includes all aspects of how the organization will shift from a legacy system to a new system. This plan covers the responsibilities associated with maintenance and support to a new contractor from the development contractor.</p>	Manager		
9	User Interface (UI) Specification	The User Interface (UI) Specification captures detailed information about the planned user interface.	Application Owner / System Manager / Requirements Team	Not yet established.	Not yet established.
10	Detailed Requirements Document	The Detailed Requirements Document captures detailed functional and non-functional requirements in the form of declarative statements. If required by the solution, this template may also be used to capture user interface specifications.	Application Owner / System Manager / Requirements Team	Not yet established.	Not yet established.
11	IT Contingency Plan	The Information Technology Contingency Plan documents the critical business functions need to be resumed and in	Information System Security Officer (ISSO)	CIO / Security and Privacy Team	Bob Ingwalson

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
		what order, what technical components are affected in the case of a disaster, and the key individuals who should be familiar with their duties under the plan.			
12	Master Test Plan (includes System Test Plan and User Acceptance Test Plan)	The Master Test Plan provides a central artifact to govern the planning and control of the test effort. It defines the general approach that will be employed to test the solution and to evaluate the results of that testing, and is the top-level plan that will be used by managers to govern and direct detailed testing activities.	Application Owner / System Manager / Test Team	CIO / Enterprise Testing Group	Karen Edwards
13	System Security Plan	The System Security Plan describes general system information such as its Federal Information Processing Standards (FIPS) 199 categorization, type of data processed, points of contact, system environment, applicable Federal laws and guidelines, and sensitivity of information processed by the system. It includes the management, operational, and technical controls required for the system. System Boundary Document and all other project related security documentation must be developed in compliance with NIST Special Publication (SP) 800-18 and SP 800-53. Further security compliance information can be found at:	Information System Security Officer (ISSO)	CIO / Security and Privacy Team	Bob Ingwalson

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
		http://csrc.nist.gov/publications/PubsSPs.html . As deemed necessary, contractors may obtain a copy of the Federal Student Aid Security Architecture Model and other security documentation by contacting their Contracting Officer post award.			
14	Configuration Management Plan	The Configuration Management (CM) Plan provides an overview of the organization, activities, overall tasks, and objectives of CM for an initiative. It addresses: baseline work products, describes the mechanism to track and control changes/change requests, and the mechanism to establish and maintain baseline integrity.	Application Owner / System Manager / Configuration Manager	CIO / Enterprise Configuration Management	Diana O'Hara
15	Preliminary Design Document	The Preliminary Design Document provides a high level design, using a number of different architectural views (to include use case diagrams) to depict different aspects of a system. It is intended to capture and convey the significant architectural decisions that have been made on the system in the early stages, allowing the high-level design to be effectively evaluated before proceeding to the detailed design stage.	Application Owner / System Manager / Development Team	CIO / Technical Architecture Support Services (TASS)	Terry Woods
16	Detailed Design Document	The Detailed Design Document provides a detailed design, using a number of different	Application Owner / System Manager /	CIO / Technical Architecture Support	Terry Woods

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
		architectural views (to include use case diagrams) to depict different aspects of the system. It is intended to capture and convey the detail necessary to allow coders to develop the system, and to support critical design reviews before beginning development.	Development Team	Services (TASS)	
17	Security Risk Assessment & Mitigation Plan	The Security Risk Assessment and Mitigation Plan provides an assessment of a system's security controls and determines the extent to which those controls have been implemented correctly - operating as intended and producing the desired outcome with respect to meeting system security requirements and a plan to mitigate findings. The security assessment also includes a list of any recommended corrective actions.	Information System Security Officer (ISSO)	CIO / Security and Privacy Team	Bob Ingwalson
18	Operations & Maintenance Plan	The Operations and Maintenance Plan documents all ongoing activities necessary to operate and maintain the system in good functioning condition. This plan includes a description of the resources required and their responsibilities, operational procedures for system startup and restart, backup and recovery, system archiving, and job scheduling. In addition, this plan addresses any training required by the user community in order to	Application Owner / System Manager / Operations and Maintenance Team	Not yet established.	Not yet established.

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
		use the system.			
19	Requirements Traceability Matrix	The Requirements Traceability Matrix associates requirements with portions of the build designed to satisfy them. Testing is also tied to the requirements on which they are based to ensure that the build meets all requirements.	Application Owner / System Manager / Requirements Team / Test Team	CIO / Enterprise Quality Assurance Team	Mike Rockis
20	Test Suites (includes cases and scripts)	Test Suites outline a set of several test scenarios, test suites, test procedures and test scripts for a component or system under test.	Application Owner / System Manager / Test Team	CIO / Enterprise Testing Group	Karen Edwards
21	Iteration Status Report	The Iteration Status Report documents the status, results and outcomes of each iteration. Note: Used for iterative development approaches.	Application Owner / System Manager / Development Team	Not yet established.	Not yet established.
22	Solution Source Code and Deployable Packages	Solution Source Code is a collection of statements or declarations written in some human-readable computer programming language.	Application Owner / System Manager / Development Team	Not yet established.	Not yet established.
23	System Test Summary Report	The Test Summary Report gives a summarization of the system test phase of the project. The report includes support materials pertaining to the software version, deviations from those areas that were agreed to in the System Test Plan, gives an overall assessment of the product that was tested, and provides an overall status of the incidents found during the system test activity.	Application Owner / System Manager / Test Team	CIO / Enterprise Testing Group	Karen Edwards

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
24	User Acceptance Test Summary Report	The User Acceptance Test Summary Report gives a summarization of the user acceptance test phase of the project. The report includes support materials pertaining to the software version, deviations from those areas that were agreed to in the User Acceptance Test Plan, gives an overall assessment of the product that was tested and gives an overall status of the incidents found during the user acceptance test.	Application Owner / System Manager / Test Team	CIO / Enterprise Testing Group	Karen Edwards
25	Production Readiness Review (PRR) Report (Report consists of Slide Presentation, PRR Checklist, and Sign-off Memo)	The Production Readiness Review is the final documented risk assessment of the release before it is put in to production.	Application Owner / System Manager	CIO / Enterprise Quality Assurance Team	Trey Wiesenburg
26	Training Plan	The Training Plan documents the training to be provided or arranged for Federal Student Aid end-users and support staff, including: prerequisites, courses, course curricula, and attendees.	Application Owner / System Manager	Not yet established.	Not yet established.
27	Solution User Manual	The Solution User Manual describes in detail the user/system interaction facilities offered by the system, which allow the users to leverage the system functionality in support of their business processes.	Application Owner / System Manager	Not yet established.	Not yet established.
28	Version Description Document	The Release Version Description Document is used to track and control versions of software and hardware being released to implementation, testing,	Application Owner / System Manager / Configuration Manager /	Not yet established.	Not yet established.

Section 1: Documentation					
This section of the PRR Checklist reviews the system documentation that is produced during the development lifecycle. It is recognized that different systems may use different names for documents and this should be explained in the comments section with the appropriate document name referenced.					
#	Document Name	Document Description	Document Author / Owner	Enterprise Guidance / Reviewer Organization	Enterprise Point of Contact
		or the final operational environment.	Development Team		
29	Security C&A and Post-Implementation Evaluation	The Security, C&A and Post-Implementation Evaluation Report documents the results of the Security, Certification and Accreditation (C&A) and Post Implementation Evaluation. The purpose of the report is to review and ensure that each general support system's and major application's security controls are implemented and/or documented in compliance with the U.S. Department of Education, U.S. Office of Management and Budget (OMB), and National Institute for Standards and Technology (NIST) guidance.	Information System Security Officer (ISSO)	CIO / Security and Privacy Team	Bob Ingwalson
30	System Retirement Plan	The System Retirement Plan describes the system retirement strategy, the solution retirement requirements list, and the data/documentation plan.	Application Owner / System Manager	Not yet established.	Not yet established.
31	System Disposal Plan	The System Disposal Plan documents the data that needs to be preserved when the system is disposed of, the timeline for the disposal activities, the software components and data to be preserved, the equipment and software disposal plan, the security measures to be taken to dispose of the system and its data, and the archival of lifecycle products.	Application Owner / System Manager	Not yet established.	Not yet established.

Section 2: Data Center Readiness

This section of the PRR Checklist reviews the activities needed to coordinate readiness of the data center to support the release moving in to the production environment.

Data Center Readiness items will primarily be coordinated by the Application Owner, System Manager, or Development Team in consultation with the Data Center's Service Management Team.

VDC Service Management Team point of contact is Wanda Broadus.

Points of contact for other data centers should be addressed to the FSA System Manager for the application that uses that data center.

Section 3: Testing

This section of the PRR Checklist reviews the testing activities that were conducted for this release.

Testing is generally assigned to a test manager or test lead by the application owner or may be assigned by CIO. System testing is generally executed by a support contractor while user acceptance testing is generally executed by Federal Student Aid personnel.

The CIO Enterprise Testing Group provides standards and coaching services for all testing activities.

The point of contact for test planning, system testing, and user acceptance testing is Karen Edwards.

The point of contact for performance testing is Terry Woods.

The point of contact for Accessibility Testing is the Department of Education/ Assistive Technology Team that conducts 508 testing is Don Barrett.

Section 4: Information System Security and Privacy

This section of the PRR Checklist reviews the status of information system security and privacy for the application and the impact of this release on information system security and privacy.

Information Security and Privacy are generally the responsibility of the Information System Security Officer for the system.

Federal Student Aid's Chief Information Officer provides policy oversight and guidance on Information Security; as well as being responsible for reporting on the security posture of Federal Student Aid's systems as required by the Federal Information Security Management Act. Additionally, for applications hosted at FSA's VDC, CIO performs security vulnerability scanning services.

Security and Privacy Team point of contact is Bob Ingwalson.

The Security Manager for the VDC is David Elliott.

The ISSO for the Virtual Data Center is John Hsu.

The data center vulnerability scanning point of contact is Rick Reyes.

Section 5: End User Support Readiness

This section of the PRR Checklist reviews the readiness of support services that are in place to support users.

Support Services Readiness is the responsibility of the application owner for end-user support functions and VDC Service Management to coordinate any support needs with the VDC.

Section 6: Communication to End Users

This section of the PRR Checklist reviews the communication of this release to end users.

Communication to end users is the responsibility of the application owner.

Appendix E – Sample Production Readiness Review Sign-Off Memo



PRR Sign-Off Memorandum

[Date]

This memorandum certifies that [system name, release number] has been reviewed by Federal Student Aid and that known risks have been disclosed to FSA Management. By signature below, Federal Student Aid accepts the risks associated with implementing this release into the production environment and allowing end-user access.

 {Name}
 System Test Lead

 Slawko Semaszczuk or designee
 CIO Virtual Data Center Manager

 {Name}
 Information System Security Officer

 Bob Ingwalson or designee
 CIO / Chief Information Security Officer (CISO)

 {Name}
 System Technical Lead

 Mike Rockis or designee
 CIO / Enterprise Quality Assurance

 {Name}
 System Owner

 Warren Gordon, Jim McMahon,
 Ganesh Reddy, or designee
 CIO Management

 {Name}
 Application/Business Owner

FSA Senior Management Sign-off is required for initial releases of major applications and integration projects. This sign-off is also required for other releases that have a significant impact on the way that FSA does business and/or interacts with a substantial end-user population.

Senior Management sign-off required by Enterprise Quality Assurance based on risk of implementing the release: Required Not Required

 {Name}
 {Title – must be Operating Committee member}

 Richard Gordon
 FSA Chief Information Officer (CIO)

Appendix F - References

Appendix F - References

This Process Description was created in accordance with the following Federal Student Aid policies:

- Clinger-Cohen Act of 1996, P.L. 104-106
- Department of Education, Department Directive OCIO: 3-105, *Procuring Electronic and Information Technology (EIT) In Conformance with Section 508 of the Rehabilitation Act of 1973*, dated 05/01/2006
- Department of Education, Department Directive OCIO: 3-108, *Information Technology Investment Management (ITIM) and Software Acquisition Policy*, dated 9/15/2006
- Department of Education, Department Directive OCIO: 1-106, *Lifecycle Management (LCM) Framework*, dated 12/2/2005
- Department of Education, Federal Student Aid, *Lifecycle Management Methodology (LMM)*
- Department of Education, Federal Student Aid, Enterprise Operational Change Management Plan, Version 1.1 (November 7, 2007)
- Department of Education, Federal Student Aid, *Enterprise Testing Standards Handbook*, Version 2.2, dated October 2, 2009
- Department of Education, Federal Student Aid, *Independent Verification & Validation Handbook*, Version 4.0, dated September 17, 2008
- Department of Education, Federal Student Aid, *Virtual Data Center Configuration Management Database Data Dictionary*, Version 1.1 (November 7, 2007)
- Federal Information Processing Standards (FIPS) 199 – *Standards for Security Categorization of Federal Information and Information Systems*
- Government Performance and Results Act of 1993, P.L. 103-62
- National Institute of Standards and Technology, Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004
- National Institute of Standards and Technology, Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009
- OMB Circular A-11 – *Preparation, Submission, and Execution of the Budget, Capital Asset Plan and Business Case*
- OMB Circular A-130 – *Management of Federal Automated Information Resources*

Appendix G – PRR Slide Template

Appendix G – PRR SLIDE TEMPLATE



[system/release name] Production Readiness Review

[date]

[These slides are provided as a guide to developing PRR presentations. It is expected that the slides will be tailored to fit the needs of particular systems. Template updated: 07-30-2010]

Agenda



- Business Background of system and this release
- Schedule
- Review of Open Risks
- Data Center Readiness
- Testing Summary
- Security & Privacy
- End User Support and Communication
- IV&V Recommendation
- Lessons Learned
- Meeting Closure

Business Background - General



[Describe the business purpose of the system in general. What major functions does this system perform for FSA?]

Business Background – Release



[Describe the business benefits that this release will provide to FSA. For example, it provides new functionality to meet a legislative requirement, improves the user experience, etc.]



High-Level Schedule Milestones

	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
Integration Testing	6/10/2008	8/10/2008
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
SDR	8/15/2008	10/15/2008
PRR	8/30/2008	10/30/2008
Production Cutover	9/1/2008	11/1/2008

Complete project schedule is available from
Jane Doe, jane.doe@ed.gov.

[Note: Milestones listed on this slide should be tailored to fit the project]



Open Risks for this release

Risk Name	Risk Description	Mitigation Strategy	Risk Owner

Data Center Readiness



- CMDB review and validation completed on 5/15/2008.
- Service Delivery Review (SDR) completed on 5/16/2008. There were no outstanding issues from the SDR [or report outstanding issues from SDR].
- Disaster recovery objectives revalidated based on this release:
 - Recovery Time Objective (RTO): [Mission Important = 48 hours or Mission Supportive = 72 hours]
 - Recovery Point Objective (RPO): [Mission Important = 24 hours or Mission Supportive = 48 hours]
- Change Request (CCM Ticket) for production implementation has been submitted to the data center. Ticket # 12345678.

Testing Summary – Test Phases



TEST PHASE	Organization Executing Tests	High Level Summary of Test Results
System Testing – Focused on testing of the entire application.	ABC Company, Development Contractor	<ul style="list-style-type: none"> Functions A and C did not perform calculations correctly. Development team fixed problems based on test findings.
Inter-system Testing – Performed by the xx team in conjunction with external entities (e.g., SSA, IRS) and internal entities (e.g., NSLDS, COD). Purpose is to test data flows and functionality between multiple systems.	ABC Company, Development Contractor and XYZ Team, O&M Contractor for other system.	<ul style="list-style-type: none"> Team considers the IST to be a success
508 Compliance testing - The 508 testing was conducted by the contractor and by the ED Chief Information Officer (CIO), Assistive Technology Team. The purpose of 508 testing is to verify system components meet Department of Education 508 compliance standards.	ED OCIO Assistive Technology Team	<ul style="list-style-type: none"> System received a "pass" rating in the report that was returned to FSA.
Performance testing – Application was tested under a load of users.	FSA- Enterprise Performance Testing Team	<ul style="list-style-type: none"> Team estimated that 5,000 concurrent users; system can handle 15,000 concurrent users within established response threshold of 2 seconds.
User Acceptance Testing – Performed by XX and YY teams. Focused on validating that major business processes work as expected.	FSA – Business Unit Users	<ul style="list-style-type: none"> Functions and A and B did not work correctly. Development team fixed problems and re-test was successful.

[Note: Please address each of the test phases included above.]

Testing Summary – Test Results



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
Performance	20	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
508 Testing	10	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
User Acceptance	100	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
TOTALS	210	20	20	20	20	80	5	5	5	5	20	5	5	5	5	20	10	10	10	10	40

Defect Severity Levels

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

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

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

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

Testing Summary – Test Results



Open Defects:

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

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

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

Security and Privacy



- ISSO is Jane Doe, confirmed by assignment memo dated 5/1/2008
- System is classified as a Minor Application
- System does not contain Personally Identifiable Information (PII).
- Confidentiality is categorized as “Low”
- Integrity is categorized as “Low”
- Availability is categorized as “Low”
- Vulnerability scans of development and test environments performed on 5/15/2008. The scans resulted in the following findings:
 - Critical: 2 findings, 2 remediated
 - High: 5 findings, 5 remediated
 - Moderate: 16 findings, 15 remediated, 1 accepted
 - Low: 48 findings, 40 remediated, 8 corrective actions scheduled
- Vulnerability scans of the production environment are scheduled for 6/15, following implementation of this release.
- The ISSO has evaluated the changes being implemented in this release and has determined that there is no impact to the security posture of the system [or state the impact if there is one].

End User Support and Comm.



- VDC Service Desk has been notified of the release to support internal teams.
- Application team help desk is aware of the release and has updated their procedures. The help desk phone number is 1-800-123-4567
- Call center scripts and procedures have been updated to support inquiries from end users. The Customer Call Center phone number is 1-800-345-6789.
- A notice will be sent to end users and posted to IFAP to notify users of the outage window and the new functionality that will be available.

IV&V Recommendation



- [IV&V Team Recommendation, if applicable.]

Lessons Learned



- Issue: [describe the background/cause of the lesson]
- Lesson: [describe the action that should be taken to address the issue on future projects]

- Issue: [describe the background/cause of the lesson]
- Lesson: [describe the action that should be taken to address the issue on future projects]

- Issue: [describe the background/cause of the lesson]
- Lesson: [describe the action that should be taken to address the issue on future projects]

Meeting Closure



- Implementation is scheduled for 6/30/2008.
- The release will be implemented during the normal maintenance window [or state outage period]
- Completion of formal sign-off memorandum
- Delivery of sign-off memorandum and supporting documentation to CIO Enterprise Quality Assurance Team