



Exchange Security



DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS for MEDICARE & MEDICAID SERVICES
Center for Consumer Information and Insurance Oversight

State Exchange Grantee Meeting September 19-20, 2011



The material in this presentation should not be viewed as having any independent legal effect, or relied upon as an interpretation or modification of the related proposed rule or statute. Not all issues or exceptions are fully addressed.

Objectives

- Review elements of security in the State Exchange **Systems**
- Discuss security guidance, procedures, and templates
- Discuss the security components of the Enterprise Life Cycle (ELC) Process and Stage Gate Success Criteria
- **Questions & Answers**



Security Elements

Minimum Security Controls for State Exchanges

Family (and Identifier)	Class	Family (and Identifier)	Class
Access Control (AC)	Technical	Incident Response (IR)	Operational
Awareness and Training (AT)	Operational	Media Protection (MP)	Operational
Audit & Accountability (AU)	Technical	Planning (PL)	Management
Security Assessment & Authorization (CA)	Management	Risk Assessment (RA)	Management
Configuration Management (CM)	Operational	System & Services Acquisition (SA)	Management
Contingency Planning (CP)	Operational	System & Communications Protection (SC)	Technical
Identification and Authentication (IA)	Technical	System and Information Integrity (SI)	Operational

The material in this presentation should not be viewed as having any independent legal effect, or relied upon as an interpretation or modification of the related proposed rule or statute. Not all issues or exceptions are fully addressed.



Security Guidance

Guidance

- CMS Harmonized Security and Privacy Framework
- •CMS Minimum Security
- **Guidance for States**
- •CMS Minimum Security
- Controls for States
- ELC Process and Success Criteria

Overview

Procedures

- System Security Plan (SSP) Procedure
- Information Security Risk
- Assessment Procedure
- Contingency Plan (CP) **Procedure**

Templates

- SSP Template
- •SSP Workbook
- Information Security

Risk Assessment

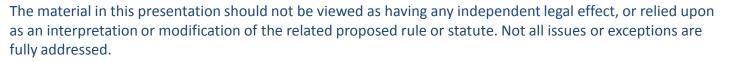
Template

Interconnection Security

Agreement (ISA)

Template

CP Template





Enterprise Life Cycle & Stage Gates

- Architectural Review
- Project Baseline Review
- Detailed Design Review
- Operational Readiness Review



Enterprise Life Cycle Security Components

Required ELC Security Artifacts

- System Security Plan
- Information Security Risk Assessment
- Contingency/Recovery Plan
- Interconnection Security Agreement

Recommended ELC Security Artifacts

- Privacy Impact Assessment
- Automated Code Review Results
- Plan of Action and Milestones (POA&M)
- Authority To Operate (ATO)
- Minimum Security Controls (Based on NIST SP 800-53, Rev 3 and NIST SP 800-53 A, Rev1)

The material in this presentation should not be viewed as having any independent legal effect, or relied upon as an interpretation or modification of the related proposed rule or statute. Not all issues or exceptions are fully addressed.



Success Criteria

Entry Evaluation Criteria

- Checklist of items that a State must meet to be ready for a review
- Any conditions / issues from a previous review are included in the entry criteria for the next review

Exit **Evaluation** Criteria

- Evaluation criteria Stage Gate Specific and Recurring Themes (Security artifacts and security controls)
- Evaluation criteria and checklist defined for each stage gate for each reviewer; 1-5 evaluation criteria per reviewer per review
- States will provide all artifacts for review 2 weeks prior to a review date
- CMS reviewers will upload initial assessment to Collaborative Application Lifecycle Tool, (CALT) 1 week before review date
- Based on scores, final review outcome is "Go", "N; Go", or "Go with Conditions"

Scoring Mechanism

- For each evaluation criteria
 - 0 = criteria not met or information provided is insufficient to make a reasonable assessment
 - 1 = information provided is satisfactory for evaluating some criteria but some questions remain
 - 2 = information provided satisfies success criteria
- Initial scores provided prior to review, no outcome / decision assigned at this time
- Final scores and outcome / decisions provided to states no later than 1 week after review

The material in this presentation should not be viewed as having any independent legal effect, or relied upon as an interpretation or modification of the related proposed rule or statute. Not all issues or exceptions are fully addressed.

