Federal Risk Management Framework (RMF) Implementation 4.0

1

About Your Instructor

Jay Ferron

CEHi, C)PTE, CWSP, CISSP, CRISC, CVEi, MCITP, MCSE, MCT, MVP, NSA-IAM…

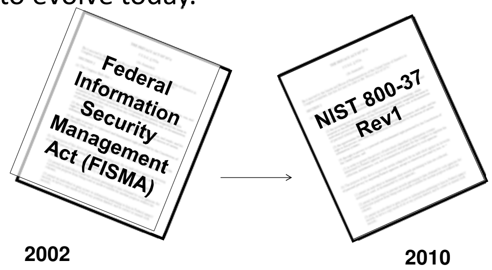
blog.mir.net

jay@ferron.com
203-675-8900

2

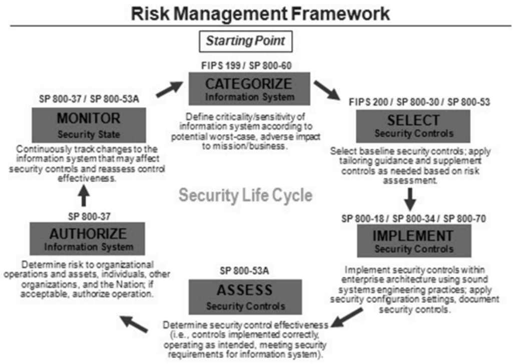
Why RMF

The following documents are the beginning of the RMF requirements as they continue to evolve today.



3

RMF Process


Risk Management Framework
Starting Point
FIPS 199 / SP 800-60
CATEGORIZE
Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.
FIPS 200 / SP 800-30 / SP 800-53
SELECT
Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.
SP 800-18 / SP 800-34 / SP 800-70
IMPLEMENT
Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings, document security controls.
SP 800-53A
ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).
SP 800-37
AUTHORIZE
Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.
SP 800-37 / SP 800-53A
MONITOR
Security State
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
Security Life Cycle

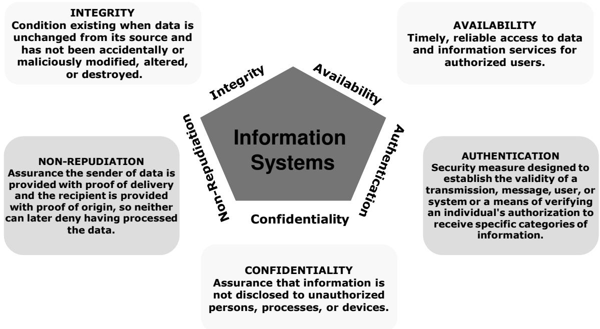
4

Assurance

- **Trusted system**:
  All protection mechanisms work to process sensitive data for many types of users and maintain the same level of protection
- **Assurance**:
  Degree of trust or confidence that the system will act in a correct and predictable manner in each and every computing situation – Confidence in the ability of the system security features to meet security objectives based on operating system, architecture, and connectivity.

5

Cybersecurity



INTEGRITY
Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

AVAILABILITY
Timely, reliable access to data and information services for authorized users.

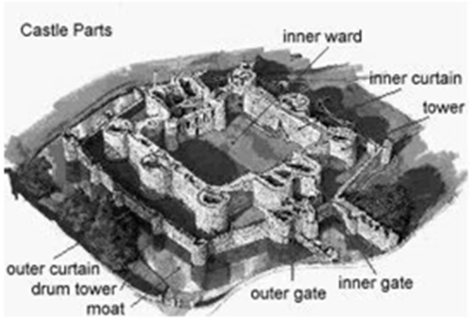
NON-REPUDIATION
Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of origin, so neither can later deny having processed the data.

AUTHENTICATION
Security measure designed to establish the validity of a transmission, message, user, or system or a means of verifying an individual's authorization to receive specific categories of information.

CONFIDENTIALITY
Assurance that information is not disclosed to unauthorized persons, processes, or devices.

6

Defense in Depth



7

Security Control Structure

Three classes of security controls.

- Management: actions taken to manage the development, maintenance, and use of the system
  - Examples: policies, procedures, rules of behavior
- Operational: day-to-day mechanisms and procedures used to protect operational systems and environment
  - Examples: awareness training, configuration management, incident response
- Technical: hardware/software controls used to provide protection of the IT system and the information it stores, processes, and/or transmits
  - Examples: access controls, authentication mechanisms, encryption

8

Management Controls

- Security Authorization and Security Control Assessments
- Planning
- Risk Assessment
- System Services and Acquisition
- Program Management
- Audit
- Human Resources

9

Operational Controls

- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Personnel Security
- System and Information Integrity

10

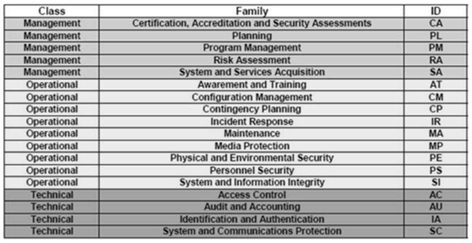
Technical Controls

- Identification and Authentication
- Access Control
- Audit and Accountability
- System and Communications Protection

11

Security Controls Structure

- Security Control Families*



Class	Family	ID
Management	Certification, Accreditation and Security Assessments	CA
Management	Planning	PL
Management	Program Management	PM
Management	Risk Assessment	RA
Management	System and Services Acquisition	SA
Operational	Awarement and Training	AT
Operational	Configuration Management	CM
Operational	Contingency Planning	CP
Operational	Incident Response	IR
Operational	Maintenance	MA
Operational	Media Protection	MP
Operational	Physical and Environmental Security	PE
Operational	Personnel Security	PS
Operational	System and Information Integrity	SI
Technical	Access Control	AC
Technical	Audit and Accounting	AU
Technical	Identification and Authentication	IA
Technical	System and Communications Protection	SC

- *Privacy Family “added” to NIST SP 800-53,rev. 4 as Appendix J.

12

Roles

- Head of Agency (CEO)
- Risk Executive (Function)
- Chief Information Officer
- Information Owner/Steward
- Senior Information Security Officer
- Authorizing Official
- Authorizing Official Designated Repr
- Common Control Provider
- Information System Owner
- Information System Security Officer
- Information Security Architect
- Information System Engineer
- Security Control Assessor

13

Head of Agency

- Highest-level senior official
- Overall responsibility for information and information systems
- Security integrated with strategic and operational processes
- Establishes appropriate accountability
- Provides active support
- Oversees monitoring

14

Head of Agency - 2

Additional Requirements for Security

- Plan for adequate security
- Assign Responsibilities
- Review Security Controls
- Authorize Processing

15

Risk Executive (Function)

- Ensures risk-related considerations are organization-wide
- Consistent across organization
- Coordinates with senior leadership to:
  - Provide comprehensive approach
  - Develop risk management strategy
  - Facilitate sharing of risk information
  - Provide forum to consider all risk sources

16

Chief Information Officer (CIO)

- Designates Senior Information Security Officer (SISO)
- Responsible for Information security policies
- Ensures adequately trained personnel
- Assists senior officials with their security responsibilities
- Allocates appropriate resources
- Responsible for FISMA reporting

17

Senior Information Security Officer (SISO)

- Carries out CIO FISMA responsibilities
- Primary liaison for CIO to organization’s senior officials
- Possesses professional qualifications
- Heads office that conducts FISMA reporting

18

Information Owner/Steward

- Authorizes specified information
- May or may not be same as system owner
- Provides input to Information System Owners
- Rules of behavior
- Single system may contain information from multiple Information Owners/Stewards

19

Authorizing Official

- Formally assumes responsibility
- Oversees budget
- Accountable for security risks
- Senior management position
- Approves Security Plan and Plan of Action and Milestone (POAM)
- Information system may involve multiple authorizing officials

20

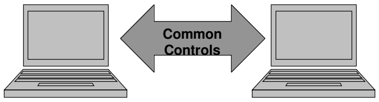
Authorizing Official Designated Representative (AODR)

- Coordinates and conducts day-to-day security activities
- May prepare final authorization package
- Does NOT make authorization decision

21

Common Control Provider

- Documents common controls in security plan (SSP)
- Validates required control assessments
- Documents assessment findings in SAR
- Produces POAMs



22

Information System Owner

- Also known as the Program Manager (8510.01)
- Focal point for Information System (IS)
- Responsible for IS throughout SDLC
- Addresses operational interests of user community
- Ensures compliance with information security requirements
- Develops and maintains SSP
- Prepares and maintains POAM
- Decides who has access to system
- Works with assessor to remediate deficiencies

23

Information System Security Officer (ISSO)

- Ensures appropriate security posture
- Serves as principal advisor to ISO
- Responsible for day-to-day security operations of system:
  - Physical and environmental
  - Personnel
  - Incident handling
  - Security training and awareness
- Policies and procedures
- Active system monitoring

24

Information Security Architect

- Adequately addresses security requirements in enterprise architecture
  - Reference models
  - Segment and solution architectures
  - Resulting information systems
- Liaison between Enterprise Architect and Information System Security Engineer
- Advisor to senior officials
  - System boundaries
  - Assessing severity of deficiencies
  - POAMs
  - Risk mitigation approaches
  - Security alerts

25

Information System Security Engineer

- Part of development team
- Employs security control best practices
- Coordinates security-related activities

Information system security engineering is the process that captures and refines information security requirements and ensures that requirements are properly integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration.

26

Security Control Assessor

- Conducts SSP assessments
- Conducts control assessments
- Provides assessment of deficiencies
- Recommends corrective action
- Prepare Security Assessment Report (SAR)
- Assessor independence:
  - Unbiased assessment process
  - Objective information for risk determination

27

Roles Overview

RMF Role	DoD	Agency	System (Operational/ Mgmt.)	System
Head of Agency	x	x		
Risk Executive (Function)	x	x		
CIO	x	x		
Information Owner/Steward	x	x	x	
SISO	x	x		
AO		x	x	
AODR		x	x	
Common Control Provider		x	x	
Information System Owner			x	
ISSO				x
Information Security Architect				x
Information System Engineer				x
Security Control Assessor				x

28

Risk Management

The process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions

Objectives:

- Achieving acceptable level of IS security
- Well-informed decisions and justifications
- Assisting in authorization decisions

29

Overview of Risk Management

- Process of balancing risk associated with business activities with adequate level of control to enable business to meet objectives.
- Holistically covers all concepts and processes affiliated with managing risk, including:
  - Systematic application of management policies, procedures, and practices
  - Tasks of communicating, consulting, establishing context
  - Identifying, analyzing, evaluating, treating, monitoring, and reviewing risk.

30

Risk Management Definition

The identification, assessment, and prioritization of risk followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of adverse events or to maximize the realization of opportunities.

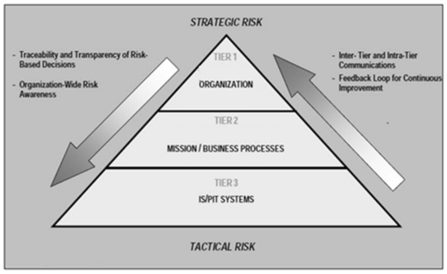
31

Responsibility vs. Accountability

- **Responsibility** belongs to those who must ensure that activities are completed successfully.
- **Accountability** applies to those who either own required resources or who have authority to approve execution or accept outcome of an activity within specific risk management processes.

32

Integrated Organization-Wide Risk Management


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
IS/PIT SYSTEMS
TACTICAL RISK

("NIST Special Publication 800-39: Managing Information Security Risk" 9)

33

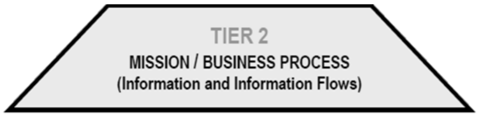
Tier 1: The Organization

- Security governance
- Techniques and methodologies
- Methods and procedures
- Mitigation measures
- Level of acceptable risk (risk tolerance)
- Ongoing monitoring

34

Tier 2: Mission/Business Process

- Defining core missions and business process
- Prioritizing missions and business processes
- Defining types of information needed
- Incorporating high-level information security into missions and business processes
- Specifying degree of autonomy

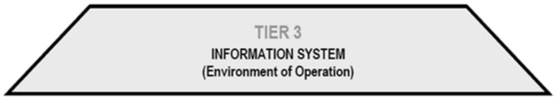

TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)

35

Tier 3: Information System

Allocation of controls

- System-specific
- Hybrid
- Common



36

Risk Assessment Process

- Step 1: Prepare for the Assessment
- Step 2: Conduct the Assessment
- Step 3: Communicate and Share Assessment Results
- Step 4: Maintain the Assessment

37

Risk Assessment Process

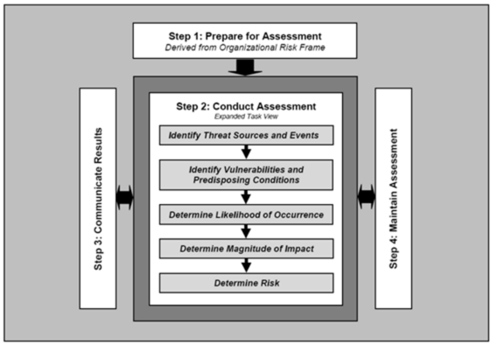
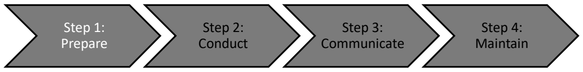

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

FIGURE 5: RISK ASSESSMENT PROCESS

38

Task 1-1: Identify Purpose

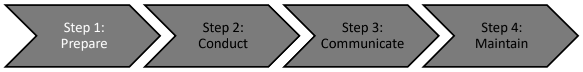
- Information that the assessment is intended to produce
- Decisions the assessment is intended to support



39

Task 1-2: Identify Scope

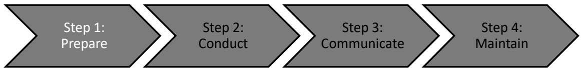
- Organizational applicability
- Time frame supported
- Architectural/technology considerations



40

Task 1-3: Identify Assumptions and Constraints

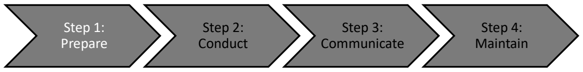
- Assumptions
- Constraints
- Risk tolerance
- Priorities/trade-offs



41

Task 1-4: Identify Information Sources

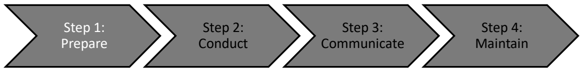
- Descriptive
- Threat
- Vulnerability
- Impact



42

Task 1-5: Identify Risk Model and Analytic Approach

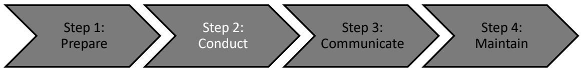
- One or more risk models for use in conducting risk assessments
- Identify which model is to be used for risk assessment



43

Task 2-1: Identify Threat Sources

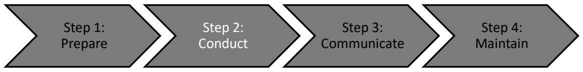
- Identify and characterize threat sources of concern
- Capability, intent and targeting characteristics for adversarial threats
- Range of effects for non-adversarial threats



44

Task 2-2: Identify Threat Events

- Potential threat events
- Relevance of the events
- Threat sources that could initiate the events



45

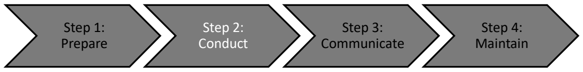
Threat Sources, Motivations, Actions

Source	Motivation	Actions
Hacker Cracker	Challenge or Ego Rebellion	Hacking, social engineering, intrusions, break-ins, unauthorized system access
Computer Criminal	Monetary Gain Unauthorized data alteration, disclosure, or destruction	Computer crime (e.g., cyber stalking), Fraudulent act (e.g., replay, impersonation, interception), Information bribery, Spoofing, System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/Terrorism, Information warfare, System attack (e.g., distributed denial of service), System penetration System tampering
Industrial Espionage	Competitive Advantage Economics	Economic exploitation, Information theft, Intrusion on personal privacy, Social engineering, System penetration, Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insider	Curiosity, Ego, Revenge Intelligence, Monetary Gain, Errors & Omissions	Employee Assault, Blackmail, Browsing of proprietary information, Computer abuse, Fraud and theft, Information bribery, Input of falsified, corrupted data, Interception, Malicious code (e.g., virus, logic bomb, Trojan horse), Sale of personal information, System bugs, System intrusion, System sabotage

46

Task 2-3: Identify Vulnerabilities and Predisposing Conditions

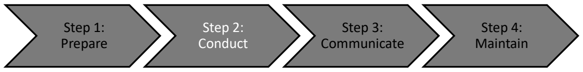
- Organizations
- Mission/business processes
- Information systems



47

Task 2-4: Determine Likelihood

- Characteristics of the threat sources
- Vulnerabilities/predisposing conditions identified
- Organizational susceptibility reflecting safeguards/countermeasures planned or implemented to impede such events



48

Task 2-4: Determine Likelihood

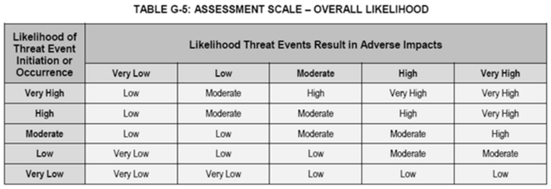
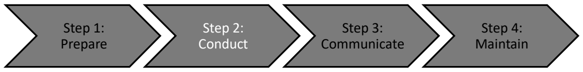


TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

("NIST Special Publication 800-30 Rev 1: Guide for Conducting Risk Assessments" Appendix G)



Step 1: Prepare

Step 2: Conduct

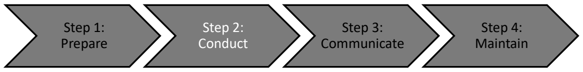
Step 3: Communicate

Step 4: Maintain

49

Task 2-5: Determine Impact

- Characteristics of threat sources
- Vulnerabilities/predisposing conditions identified
- Organizational susceptibility reflecting safeguards/countermeasures planned or implemented to impede such events



Step 1: Prepare

Step 2: Conduct

Step 3: Communicate

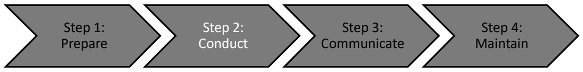
Step 4: Maintain

50

Task 2-5: Determine Impact

Qualitative Values	Semi-Quantitative Values		Description (paraphrased)
Very High	96-100	10	Expected to have **multiple** severe or catastrophic effects
High	80-95	8	Expected to have severe or catastrophic effects
Moderate	21-79	5	Expected to have serious effects
Low	5-20	2	Expected to have limited effects
Very Low	0-4	0	Expected to have negligible effects

("NIST Special Publication 800-30 Rev 1: Guide for Conducting Risk Assessments" Appendix H)



Step 1: Prepare

Step 2: Conduct

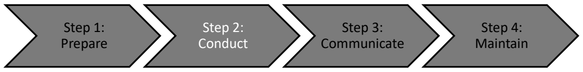
Step 3: Communicate

Step 4: Maintain

51

Task 2-5: Determine Risk

- Impact that would result from events
- Likelihood of events occurring



Step 1: Prepare

Step 2: Conduct

Step 3: Communicate

Step 4: Maintain

52

Task 3-1: Communicate Risk Assessment Results

- Organizational decision makers
- Support risk responses

Step 1: Prepare

Step 2: Conduct

Step 3: Communicate

Step 4: Maintain

53

Task 3-2: Share Risk-Related Results

- Organizational decision makers
- Support risk responses

Step 1: Prepare

Step 2: Conduct

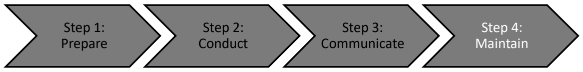
Step 3: Communicate

Step 4: Maintain

54

Task 4-1: Monitor Risk Factors

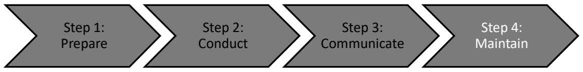
- Organizational operations and assets
- Individuals
- Other organizations
- The Nation



55

Task 4-2: Update Risk Assessment

- Organizational operations and assets
- Individuals
- Other organizations
- The Nation



56

Risk Response Options

- Risk Avoidance
- Risk Mitigation
- Risk Sharing or Transfer
- Risk Acceptance

First three can be in any order, but Risk Acceptance is always last option.

57

Risk Assessment Report

- Many templates available
- No one format is defined – organizationally-dependent

58

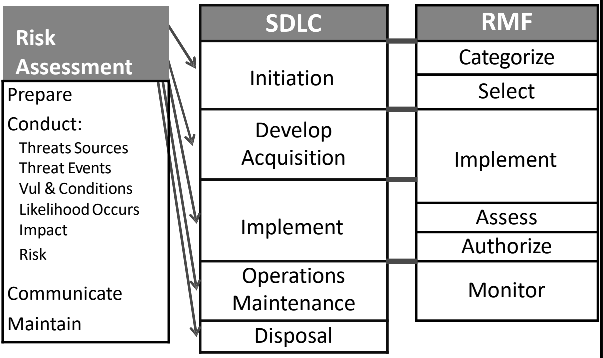
Risk Assessment and RMF

When are Risk Assessments conducted under RMF in accordance with SP 800-30, rev. 1?

- Step 2 – Selection of Controls
- Step 4 – Assessment of System and Controls
- Step 6 – Task 2 - Reassessment of System & Controls
- At any point when new risks have been identified & need mitigation

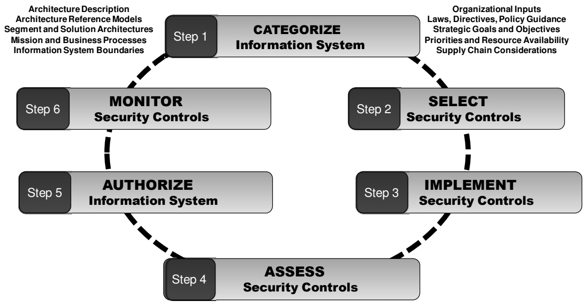
59

Risk Assessment and the SDLC



60

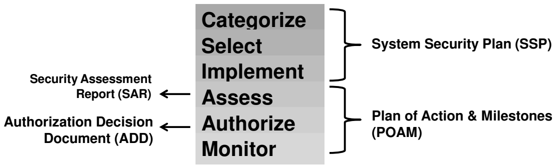
RMF: The Process


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

61

Key Documents Produced


Categorize
Select
Implement
Assess
Authorize
Monitor
System Security Plan (SSP)
Security Assessment Report (SAR)
Authorization Decision Document (ADD)
Plan of Action & Milestones (POAM)

Additional artifacts (supporting documentation) may be required.

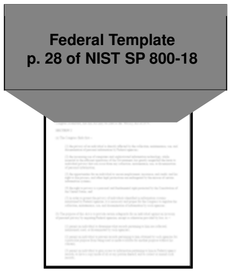
62

Step 1: Categorize Information System

1. Task 1-1 Security Categorization
2. Task 1-2 Information System Description
3. Task 1-3 Information System Registration

63

Sample SSP


Federal Template
p. 28 of NIST SP 800-18

64

Where is system categorization documented?

- System Security Plan
  - NIST SP 800-18
- System Owner/PM responsibility
- Basic Outline includes:
  - Description
  - POCs
  - Listing of Controls
  - Approvals
  - Artifacts

65

What gets documented in SSP?

- Mission, Vision of System
- Duty responsibilities and POCs
- System Description and Boundaries
- Security baseline of Security Controls
- Status of these controls
- Approvals
- Appendixes

66

SSP Elements - 1

System Security Plan Elements	Description
System Name and Identifier	The first item listed in the system security plan is the system name and identifier. Each system should be assigned a name and unique identifier.
System Categorization	Each system identified in the agency's system inventory must be categorized using FIPS 199. NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, provides implementation guidance in completing this activity.
System Owner	A designated system owner must be identified in the system security plan for each system. This person is the key point of contact (POC) for the system and is responsible for coordinating system development life cycle (SDLC) activities specific to the system. It is important that this person have expert knowledge of the system capabilities and functionality. The assignment of a system owner should be documented in writing and the plan should include the following contact information: • Name • Title • Agency • Address • Phone Number • Email Address

67

SSP Elements - 2

System Security Plan Elements	Description
Authorizing Official	An authorizing official must be identified in the system security plan for each system. This person is the senior management official who has the authority to authorize operation (accredit) of an information system (major application or general support system) and accept the residual risk associated with the system.
Other Designated Contacts	This section should include names of other key contact personnel who can address inquiries regarding system characteristics and operation.
Assignment of Security Responsibility	Within an agency, an individual must be assigned responsibility for each system. This can be accomplished in many ways. In some agencies, the overall responsibility may be delegated to the SISO.
System Operational Status	Indicate one or more of the following for the system's operational status. If more than one status is selected, list which part of the system is covered under each status:
	• *Operational* — the system is in production
	• *Under Development* — the system is being designed, developed, or implemented.
	• *Undergoing a major modification* — the system is undergoing a major conversion or transition.

68

SSP Elements - 3

System Security Plan Elements	Description
Information System Type	Define system as a major application or general support system.
General Description/Purpose	Prepare a brief description (one to three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an agency, business census data analysis, crop reporting support).
System Environment	Provide a brief (one to three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as use of remote access, wireless technology, VoIP, etc.
System Interconnection/Information Sharing	System interconnection is the direct connection of two or more IT systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit.

69

SSP Elements - 4

System Security Plan Elements	Description
Laws, Regulations, and Policies Affecting the System	List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of the system and information retained by Agency. The SSP will document the level of laws, regulations, and policies effecting Agency's system.
Security Control Selection	In preparation for documenting how the NIST SP 800-53 security controls for the applicable security control baseline (low-, moderate-, or high impact information systems) are implemented or planned to be implemented, the security controls contained in the baseline should be reviewed and possibly tailored.
Minimum Security Controls	How that the security controls have been selected, tailored, and the common controls identified, describe each control.
Completion and Approval Dates	The completion date of the system security plan should be provided. The completion date should be updated whenever the plan is periodically reviewed and updated. When the system is updated, a version number should be added. The system security plan should also contain the date the authorizing official approved the plan.

70

SSP Elements - 5

System Security Plan Elements	Description
Ongoing System Security Plan Maintenance	Once the information system security plan is developed, it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system.

71

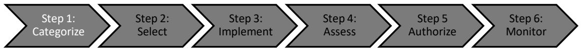
Step 1 – Categorization Walk-Through

The following slides walk you through the Step 1 – Categorization process. Each subtask is broken down with the specific roles and responsibilities, inputs, outputs and required actions.

72

Task 1-1: Security Categorization

Task 1-1	**Security Categorization** • Confidentiality, Integrity, Availability • Low, Moderate, Hight
Documents	System Security Plan
Roles	Information System Owner Information Owner/Steward
SDLC	Initiation (concept/requirements definition)



73

Initial Stakeholder Meeting

Task 1-1 | Security Categorization

- Chief Information Officer (CIO)
- Senior Information Security Officer (SISO)
- Authorizing Official/AODR
- CDSO (Cross Domain Solutions Office) Representative – If needed
- Risk Executive
- Information System Owner/PM Office
- ISSO/ISSE/ISSM
- User Representatives
- Independent Evaluation Element

74

Information Necessary for Categorization

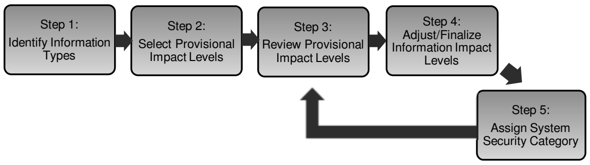
Task 1-1 | Security Categorization

Unique identifier	Information flows
System Owner/contact information	Organizational mission (s) – Codified in US law
Governing organization	System users
Location of system	System operation
Purpose, function, capabilities	Interconnection of systems
Types of information to be processed	Security authorization/ Termination dates
Security Category	Security authorization process roles
Boundary of system	Acquisition/SDLC status
Architectural description/ Network topology	Hardware/ Firmware/ Software

75

Task 1-1: Categorization Process

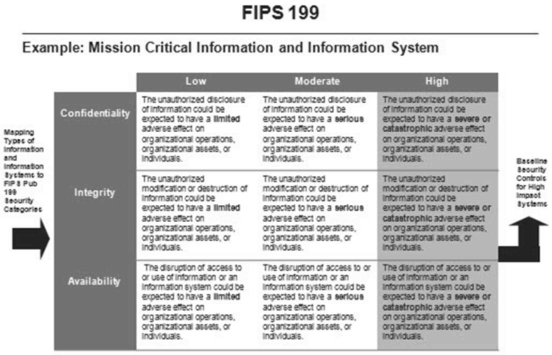
Task 1-1 | Security Categorization



Step 1: Identify Information Types
Step 2: Select Provisional Impact Levels
Step 3: Review Provisional Impact Levels
Step 4: Adjust/Finalize Information Impact Levels
Step 5: Assign System Security Category

76

FIPS 199 Example



FIPS 199

Example: Mission Critical Information and Information System

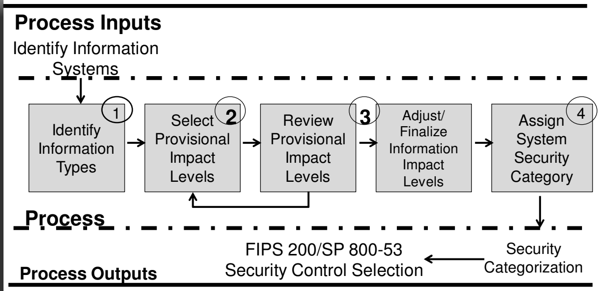
	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Mapping Types of Information and Information Systems to FIPS Pub 199 Security Categories
Baseline Security Controls for High Impact Systems

77

Assignment of Impact Levels and Security Categorization

Task 1-1 | Security Categorization



Process Inputs
Identify Information Systems
Identify Information Types
1
Select Provisional Impact Levels
2
Review Provisional Impact Levels
3
Adjust/ Finalize Information Impact Levels
Assign System Security Category
4
Process
Process Outputs
FIPS 200/SP 800-53 Security Control Selection
Security Categorization

78

FIPS-199/SP800-60 Step 1

Identify Information Types in system

- Information System-based first
  - Mission Critical
  - Mission Essential
  - Mission Support/Administrative

79

FIPS-199/SP800-60 Step 1

Identify Information Types in system

- Information-based second
  - Privacy
  - Medical
  - Proprietary
  - Financial
  - Trade Secrets
  - Contractor Sensitive
  - Investigative
  - Etc.

80

FIPS-199/SP800-60 Step 2

Select Provisional Impacts

- Impact for each Information Type identified
- Security Category (SC) determined
- Written as:

  SC info type = {(confidentiality, impact), (integrity, impact), (availability, impact)}

81

FIPS-199/SP800-60 Step 3

- Review provisional impacts appropriateness based upon:
  - Organization
  - Environment
  - Mission
  - Use
  - Data Sharing requirements
- Adjust impact levels based upon:
  - Security objectives
  - Operational drivers
  - Situational drivers

82

FIPS-199/SP800-60 Step 4

- Select the impact level high water mark for each objective:
  - Confidentiality = high, moderate, low, N/A
  - Integrity = high, moderate, low
  - Availability = high, moderate, low
- Assign system level high water mark based on aggregate of all Impact Levels

83

Potential Impacts

Task 1-1 › Security Categorization

Information Types:

- **Personally Identifiable Information** – Moderate Impact
- **Protected Health Information** – Moderate to High Confidentiality Impact
- **Trade Secrets** – Moderate Impact
- **System Information** –
  Impact Level Commensurate to the Information being processed

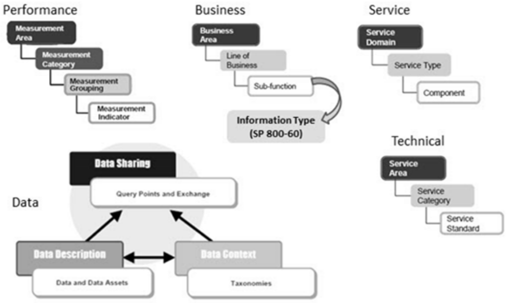
Other System Factors:

- **Public Information Integrity**—Low or Moderate Integrity Impact
- **Catastrophic Loss of System Availability**—High Availability Impact
- **Supporting and Interconnecting Systems**—
  Use the high water mark for the system being supported
- **Critical Infrastructures and Key Resources**—
  Based on the security level of the mission served

84

FEA Information Types

Task 1-1 › Security Categorization



85

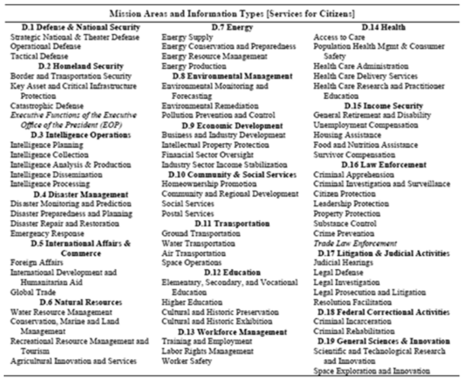
Identifying Information Types

Task 1-1 › Security Categorization

- OMB's business reference model:
  - Basis for identifying information types
  - Four business areas/ 39 lines of business
- Mission based information types:
  - Service for citizens (purpose of gov't)
  - Mode of delivery (to achieve purpose)
- Management & support information types:
  - Support delivery of services (necessary operational support)
  - Management of government resources (resource management functions)

86

Mission Areas/Information Types



Mission Areas and Information Types [Services for Citizens]

D.1 Defense & National Security
Strategic National & Theater Defense
Operational Defense
Tactical Defense

D.2 Homeland Security
Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
Executive Functions of the Executive Office of the President (EOP)

D.3 Intelligence Operations
Intelligence Planning
Intelligence Collection
Intelligence Analysis & Production
Intelligence Dissemination
Intelligence Processing

D.4 Disaster Management
Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response

D.5 International Affairs & Commerce
Foreign Affairs
International Development and Humanitarian Aid
Global Trade

D.6 Natural Resources
Water Resource Management
Conservation, Marine and Land Management
Recreational Resource Management and Tourism
Agricultural Innovation and Services

D.7 Energy
Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

D.8 Environmental Management
Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

D.9 Economic Development
Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
Industry Sector Income Stabilization

D.10 Community & Social Services
Homeownership Promotion
Community and Regional Development
Social Services
Postal Services

D.11 Transportation
Ground Transportation
Water Transportation
Air Transportation
Space Operations

D.12 Education
Elementary, Secondary, and Vocational Education
Higher Education
Cultural and Historic Preservation
Cultural and Historic Exhibition

D.13 Workforce Management
Training and Employment
Labor Rights Management
Worker Safety

D.14 Health
Access to Care
Population Health Mgmt & Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

D.15 Income Security
General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

D.16 Law Enforcement
Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
Trade Law Enforcement

D.17 Litigation & Judicial Activities
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation

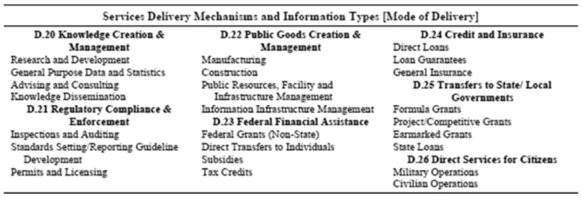
D.18 Federal Correctional Activities
Criminal Incarceration
Criminal Rehabilitation

D.19 General Sciences & Innovation
Scientific and Technological Research and Innovation
Space Exploration and Innovation

87

Service Delivery Information Types

Task 1-1 › Security Categorization



Services Delivery Mechanisms and Information Types [Mode of Delivery]

D.20 Knowledge Creation & Management
Research and Development
General Purpose Data and Statistics
Advising and Consulting
Knowledge Dissemination

D.21 Regulatory Compliance & Enforcement
Inspections and Auditing
Standards Setting/Reporting Guideline Development
Permits and Licensing

D.22 Public Goods Creation & Management
Manufacturing
Construction
Public Resources, Facility and Infrastructure Management
Information Infrastructure Management

D.23 Federal Financial Assistance
Federal Grants (Non-State)
Direct Transfers to Individuals
Subsidies
Tax Credits

D.24 Credit and Insurance
Direct Loans
Loan Guarantees
General Insurance

D.25 Transfers to State/ Local Governments
Formula Grants
Project/Competitive Grants
Earmarked Grants
State Loans

D.26 Direct Services for Citizens
Military Operations
Civilian Operations

88

Service Delivery Information Types

Task 1-1 › Security Categorization

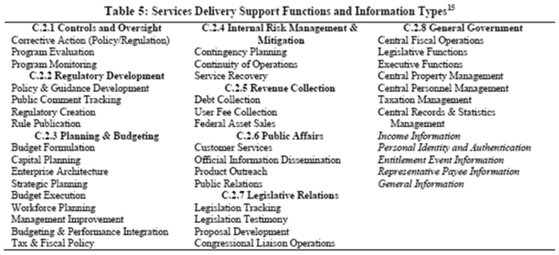


Table 5: Services Delivery Support Functions and Information Types[15]

C.2.1 Controls and Oversight
Corrective Action (Policy/Regulation)
Program Evaluation
Program Monitoring

C.2.2 Regulatory Development
Policy & Guidance Development
Public Comment Tracking
Regulatory Creation
Rule Publication

C.2.3 Planning & Budgeting
Budget Formulation
Capital Planning
Enterprise Architecture
Strategic Planning
Budget Execution
Workforce Planning
Management Improvement
Budgeting & Performance Integration
Tax & Fiscal Policy

C.2.4 Internal Risk Management & Mitigation
Contingency Planning
Continuity of Operations
Service Recovery

C.2.5 Revenue Collection
Debt Collection
User Fee Collection
Federal Asset Sales

C.2.6 Public Affairs
Customer Services
Official Information Dissemination
Product Outreach
Public Relations

C.2.7 Legislative Relations
Legislation Tracking
Legislation Testimony
Proposal Development
Congressional Liaison Operations

C.2.8 General Government
Central Fiscal Operations
Legislative Functions
Executive Functions
Central Property Management
Central Personnel Management
Taxation Management
Central Records & Statistics Management
Income Information
Personal Identity and Authentication
Entitlement Event Information
Representative Payee Information
General Information

89

Resource Mgmt Information Types

Task 1-1 › Security Categorization

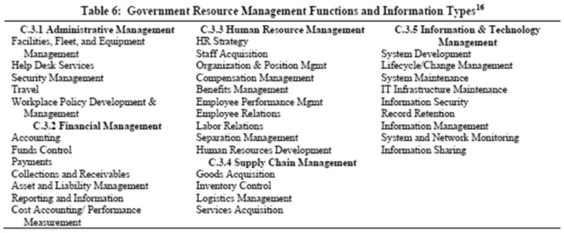


Table 6: Government Resource Management Functions and Information Types[16]

C.3.1 Administrative Management
Facilities, Fleet, and Equipment Management
Help Desk Services
Security Management
Travel
Workplace Policy Development & Management

C.3.2 Financial Management
Accounting
Funds Control
Payments
Collections and Receivables
Asset and Liability Management
Reporting and Information
Cost Accounting/ Performance Measurement

C.3.3 Human Resource Management
HR Strategy
Staff Acquisition
Organization & Position Mgmt
Compensation Management
Benefits Management
Employee Performance Mgmt
Employee Relations
Labor Relations
Separation Management
Human Resources Development

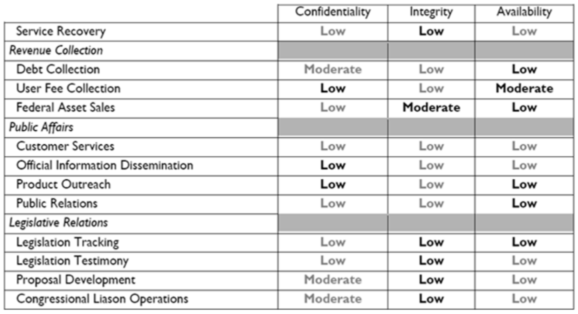
C.3.4 Supply Chain Management
Goods Acquisition
Inventory Control
Logistics Management
Services Acquisition

C.3.5 Information & Technology Management
System Development
Lifecycle/Change Management
System Maintenance
IT Infrastructure Maintenance
Information Security
Record Retention
Information Management
System and Network Monitoring
Information Sharing

90

Info Types & Impact Mgmt & Support

Task 1-1 | Security Categorization

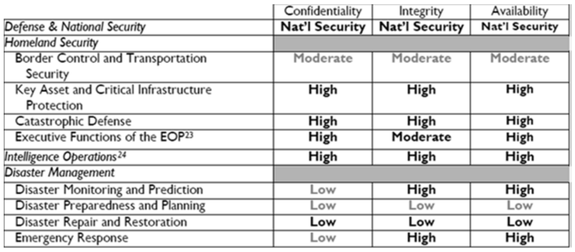


	Confidentiality	Integrity	Availability
Service Recovery	Low	**Low**	Low
Revenue Collection			
Debt Collection	Moderate	Low	**Low**
User Fee Collection	**Low**	Low	**Moderate**
Federal Asset Sales	Low	**Moderate**	**Low**
Public Affairs			
Customer Services	Low	Low	Low
Official Information Dissemination	**Low**	Low	Low
Product Outreach	**Low**	Low	**Low**
Public Relations	Low	Low	**Low**
Legislative Relations			
Legislation Tracking	Low	**Low**	**Low**
Legislation Testimony	Low	**Low**	Low
Proposal Development	Moderate	**Low**	Low
Congressional Liason Operations	Moderate	**Low**	Low

91

Info Types & Impact: Mission Specific

Task 1-1 | Security Categorization



	Confidentiality	Integrity	Availability
Defense & National Security	**Nat'l Security**	**Nat'l Security**	**Nat'l Security**
Homeland Security			
Border Control and Transportation Security	Moderate	Moderate	Moderate
Key Asset and Critical Infrastructure Protection	**High**	**High**	**High**
Catastrophic Defense	**High**	**High**	**High**
Executive Functions of the EOP[23]	**High**	**Moderate**	**High**
Intelligence Operations[24]	**High**	**High**	**High**
Disaster Management			
Disaster Monitoring and Prediction	Low	**High**	**High**
Disaster Preparedness and Planning	Low	Low	Low
Disaster Repair and Restoration	**Low**	**Low**	**Low**
Emergency Response	Low	**High**	**High**

92

FIPS 199 Categorization Examples

Task 1-1 | Security Categorization

System Component	Confidentiality	Integrity	Availability
Contract Information	MOD	MOD	LOW
Administrative Information	LOW	LOW	LOW
Information System	MOD	MOD	LOW

What is the resulting rating for the overall system?

("NIST Special Publication 800-60 Volume I Revision 1: Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories" 25-26)

93

FIPS 199 Categorization Examples

Task 1-1 | Security Categorization

System Component	Confidentiality	Integrity	Availability
Sensor Data	N/A	HIGH	HIGH
Administrative Information	LOW	LOW	LOW
Information System	LOW	HIGH	HIGH

"NIST Special Publication 800-60 Volume I Revision 1: Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories" 25-26

94

Guidelines for Adjusting System Categorization

Task 1-1 | Security Categorization

- Aggregation
- Critical System Functionality
- Extenuating Circumstances
- External Factors
- Public Information Integrity
- Critical Infrastructures and Key Resources
- Trade Secrets
- Overall Information System Impact
- Privacy Information

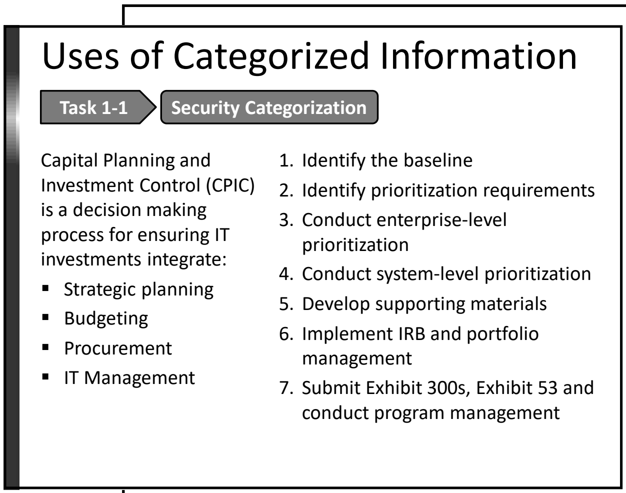
95

Other Considerations

Task 1-1 | Security Categorization

- Aggregation
  - Combinations of data which increase CIA
  - "Total is > the sum of the parts"
  - Especially prevalent in PII and HIPAA areas
- Criticality
  - Impact on connected systems – both connected to and receiving from systems

96



Uses of Categorized Information

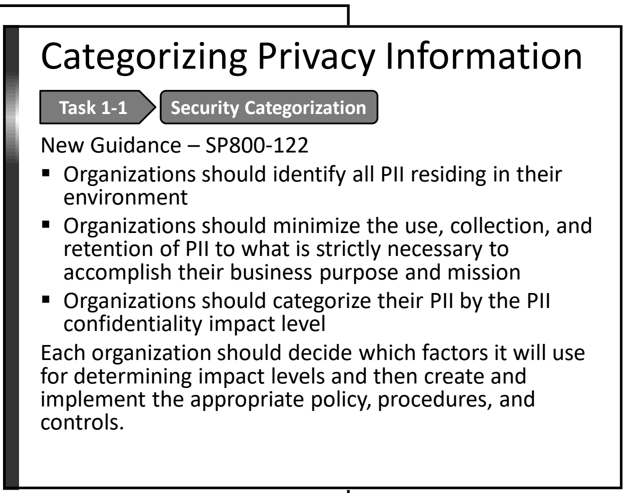
Task 1-1 Security Categorization

Capital Planning and Investment Control (CPIC) is a decision making process for ensuring IT investments integrate:

- Strategic planning
- Budgeting
- Procurement
- IT Management

1. Identify the baseline
2. Identify prioritization requirements
3. Conduct enterprise-level prioritization
4. Conduct system-level prioritization
5. Develop supporting materials
6. Implement IRB and portfolio management
7. Submit Exhibit 300s, Exhibit 53 and conduct program management

97



Categorizing Privacy Information

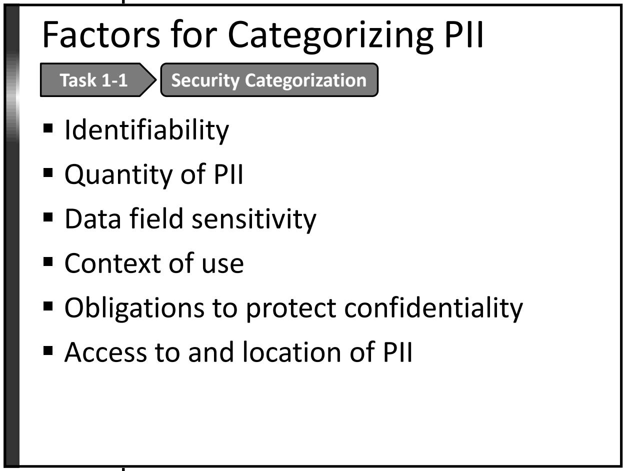
Task 1-1 Security Categorization

New Guidance – SP800-122

- Organizations should identify all PII residing in their environment
- Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission
- Organizations should categorize their PII by the PII confidentiality impact level

Each organization should decide which factors it will use for determining impact levels and then create and implement the appropriate policy, procedures, and controls.

98

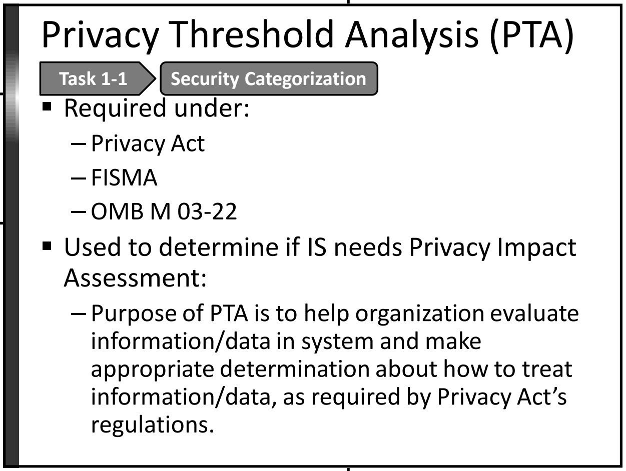


Factors for Categorizing PII

Task 1-1 Security Categorization

- Identifiability
- Quantity of PII
- Data field sensitivity
- Context of use
- Obligations to protect confidentiality
- Access to and location of PII

99

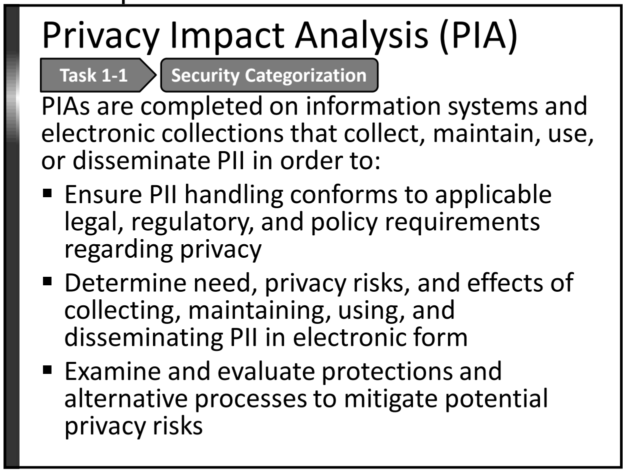


Privacy Threshold Analysis (PTA)

Task 1-1 Security Categorization

- Required under:
  - Privacy Act
  - FISMA
  - OMB M 03-22
- Used to determine if IS needs Privacy Impact Assessment:
  - Purpose of PTA is to help organization evaluate information/data in system and make appropriate determination about how to treat information/data, as required by Privacy Act's regulations.

100



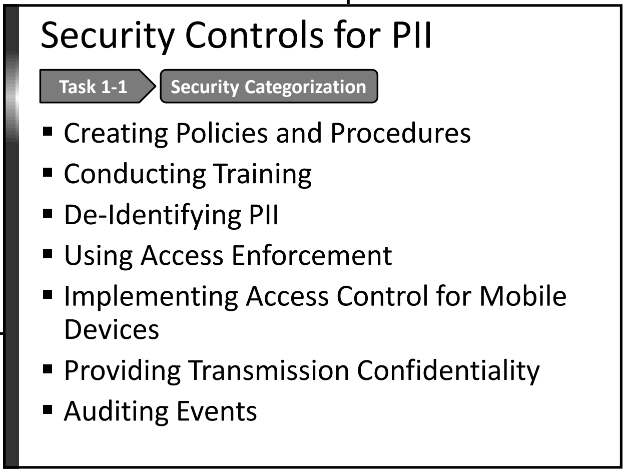
Privacy Impact Analysis (PIA)

Task 1-1 Security Categorization

PIAs are completed on information systems and electronic collections that collect, maintain, use, or disseminate PII in order to:

- Ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy
- Determine need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form
- Examine and evaluate protections and alternative processes to mitigate potential privacy risks

101



Security Controls for PII

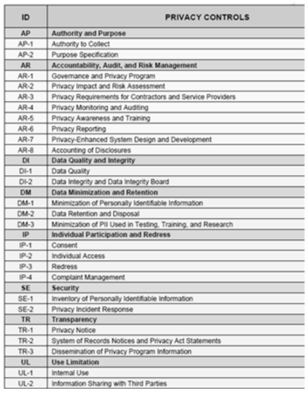
Task 1-1 Security Categorization

- Creating Policies and Procedures
- Conducting Training
- De-Identifying PII
- Using Access Enforcement
- Implementing Access Control for Mobile Devices
- Providing Transmission Confidentiality
- Auditing Events

102

Privacy Controls by Family

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

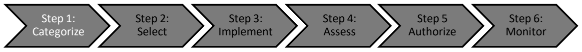


ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

103

Task 1-2: Information System Description

Task 1-2	**Information System Description** • **Level of detail determined by security categorization**
Documents	System Security Plan
Roles	Information System Owner
SDLC	Initiation (concept/requirements definition)



104

Information System Boundaries

Task 1-2 | Information System Description

Defined by set of information resources allocated to system:

- Support same mission/business objectives
- Reside in same operating environment

Boundary Size	Advantage	Disadvantage
Too expansive	Fewer documents	• Unwieldy • Complex • Creates conflict
Too limited	Focused	• More to manage • Inflates cost • Possible gaps

105

Information System Boundaries

Task 1-2 | Information System Description

- Establishing Information System Boundaries
- Boundaries for Complex Information Systems
- Changing Technologies and Effect on Information System Boundaries

106

Changing Technologies Effect on Boundaries

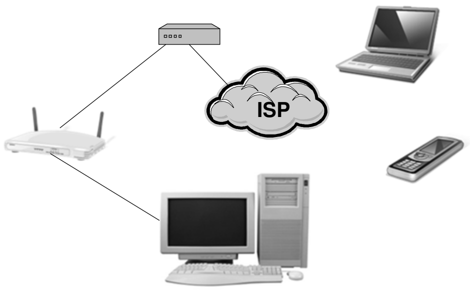
Task 1-2 | Information System Description

- Dynamic Subsystems
  - Net-centric
  - Service-oriented Architecture
  - Cloud Computing
- External Subsystems
  - Contractor Systems
  - Government Owned – Contractor Operated (GOCO)

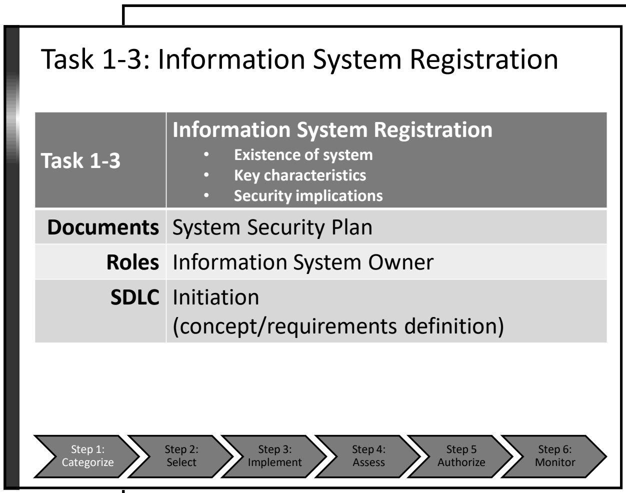
107

Standalone Environments

Task 1-2 | Information System Description



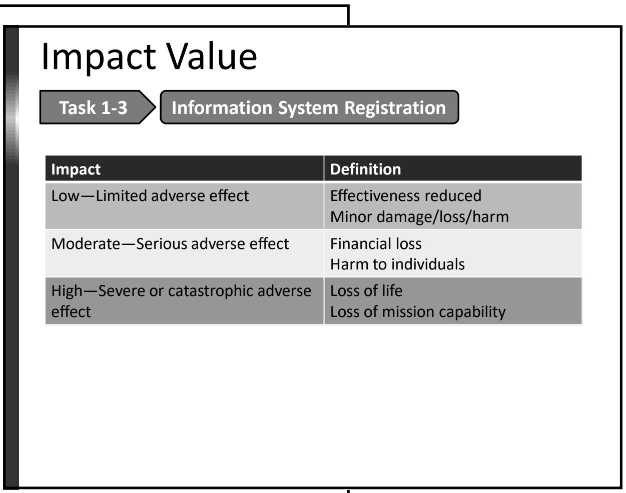
108



Task 1-3: Information System Registration

Task 1-3	**Information System Registration** • Existence of system • Key characteristics • Security implications
Documents	System Security Plan
Roles	Information System Owner
SDLC	Initiation (concept/requirements definition)

109

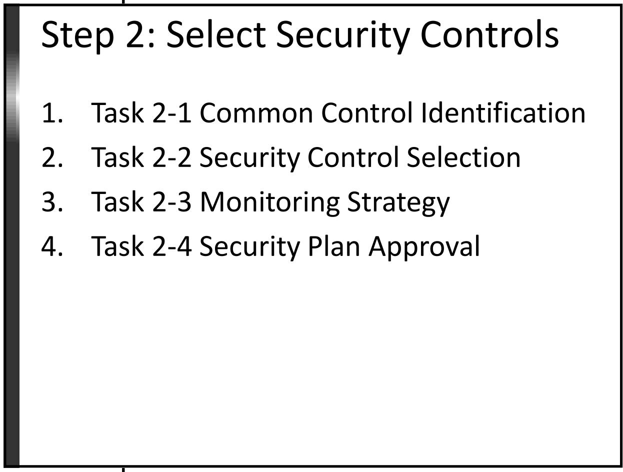


Impact Value

Task 1-3 Information System Registration

Impact	Definition
Low—Limited adverse effect	Effectiveness reduced Minor damage/loss/harm
Moderate—Serious adverse effect	Financial loss Harm to individuals
High—Severe or catastrophic adverse effect	Loss of life Loss of mission capability

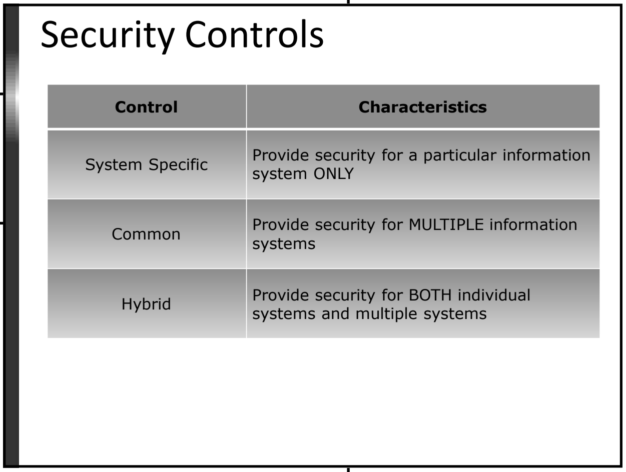
110



Step 2: Select Security Controls

1. Task 2-1 Common Control Identification
2. Task 2-2 Security Control Selection
3. Task 2-3 Monitoring Strategy
4. Task 2-4 Security Plan Approval

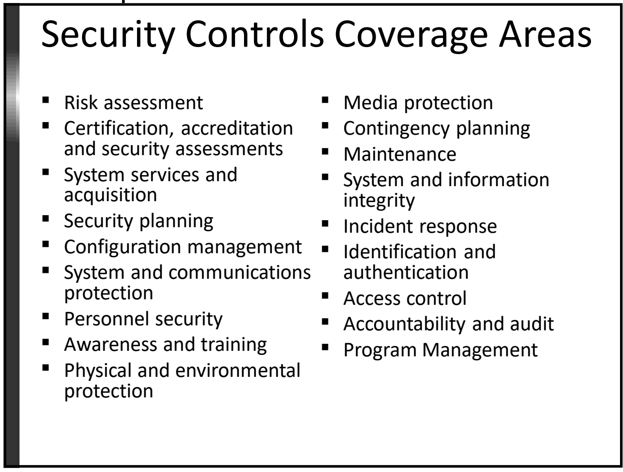
111



Security Controls

Control	Characteristics
System Specific	Provide security for a particular information system ONLY
Common	Provide security for MULTIPLE information systems
Hybrid	Provide security for BOTH individual systems and multiple systems

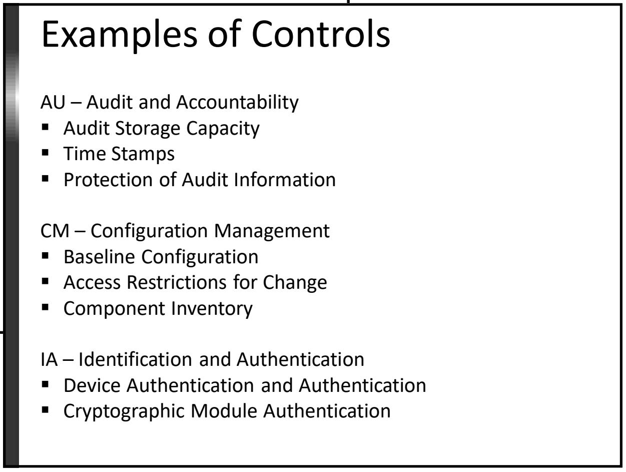
112



Security Controls Coverage Areas

- Risk assessment
- Certification, accreditation and security assessments
- System services and acquisition
- Security planning
- Configuration management
- System and communications protection
- Personnel security
- Awareness and training
- Physical and environmental protection
- Media protection
- Contingency planning
- Maintenance
- System and information integrity
- Incident response
- Identification and authentication
- Access control
- Accountability and audit
- Program Management

113



Examples of Controls

AU – Audit and Accountability

- Audit Storage Capacity
- Time Stamps
- Protection of Audit Information

CM – Configuration Management

- Baseline Configuration
- Access Restrictions for Change
- Component Inventory

IA – Identification and Authentication

- Device Authentication and Authentication
- Cryptographic Module Authentication

114

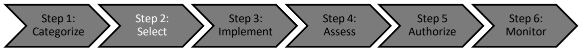
Step 2: Selection

The following slides walk you through the Step 2 – Selection process. Each subtask is broken down with the specific roles and responsibilities, inputs, outputs and required actions.

115

Task 2-1: Common Control Identification

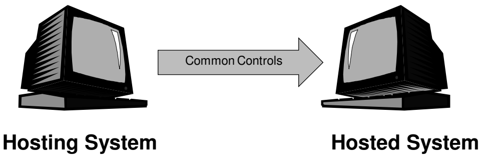
Task 2-1	**Common Control Identification** • Determine sufficient & adequate protection • Supplement with system specific or hybrid • Accept greater risk
Documents	System Security Plan
Roles	Chief Information Officer Chief Information Security Officer Information Security Architect Common Control Provider
SDLC	Initiation (concept/requirements definition)



116

Common Controls

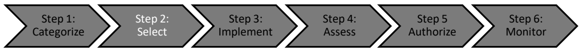
Common controls are provided by the hosting system.



117

Task 2-2: Select Security Controls

Task 2-2	**Select Security Controls** • Baseline controls • Tailor baseline controls • Supplement tailored controls • Minimum assurance
Documents	System Security Plan
Roles	Information Security Architect Information System Owner
SDLC	Initiation (concept/requirements definition)

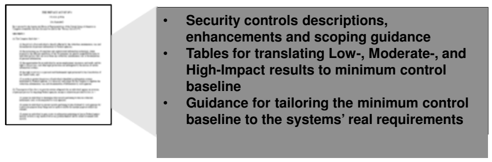


118

Baseline Controls

Task 2-2 | Select Security Controls

NIST SP 800-53



- Security controls descriptions, enhancements and scoping guidance
- Tables for translating Low-, Moderate-, and High-Impact results to minimum control baseline
- Guidance for tailoring the minimum control baseline to the systems' real requirements

119

Control Definition

Task 2-2 | Select Security Controls

Controls are the policies, procedures, practices and guidelines designed to provide reasonable assurance that:

- Business objectives are achieved.
- Undesired events are prevented or detected and corrected.

120

Defense in Depth – Layered Defense

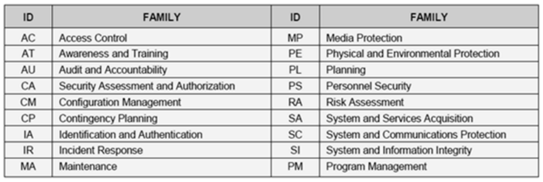
Task 2-2 Select Security Controls

Deploy a combination of controls so if one control fails, another control prevents total compromise of system and restricts access to protected assets.

121

Security Control Identifiers & Family Names

Task 2-2 Select Security Controls

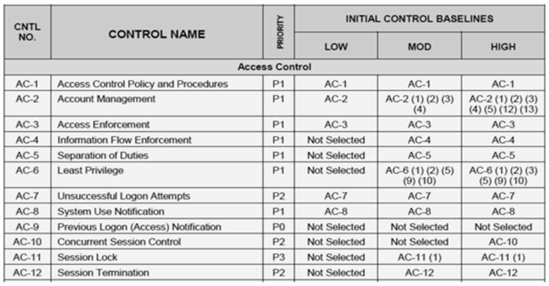


ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

122

SP 800-53 Appendix D

Task 2-2 Select Security Controls

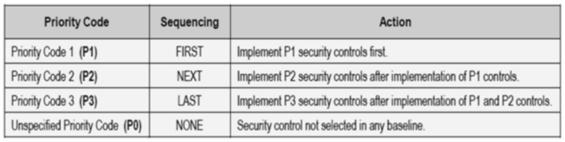


CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12

123

Security Control Prioritization Codes

Task 2-2 Select Security Controls



Priority Code	Sequencing	Action
Priority Code 1 **(P1)**	FIRST	Implement P1 security controls first.
Priority Code 2 **(P2)**	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 **(P3)**	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code **(P0)**	NONE	Security control not selected in any baseline.

Security Control Prioritization
1. Not used in DOD
2. Installation priority only in Federal civilian systems

124

Control Selection Criteria

Task 2-2 Select Security Controls

Minimum security baseline is starting point – where from? Tailoring of controls accomplished through:

- Scoping
- Parameterization
- Compensating guidance

Supplementing through additional controls is next using enhancements in SP 800-53 Sets of Controls. Additional Criteria:

- Operating environment
- Organizational-specific requirements
- Threat assessments
- CBA for implementation of controls

125

Control Categories

Task 2-2 Select Security Controls

Primary:

- Preventive
- Detective
- Corrective

Secondary:

- Supplemental
- Compensating
- Deterrent

126

Kinds of Controls

Task 2-2 › Select Security Controls

- Common
  - Control that is inherited by one or more organizational information systems
- Hybrid
  - Control that is implemented in part as common and in part as system-specific
- System-Specific
  - Control that is implemented entirely within the information system under review

127

Types of Controls

Task 2-2 › Select Security Controls

- Technical focus
  - AC, AU, IA, SC
- Management focus
  - CA, PL, PM, RA, SA
- Operational Focus
  - AT, CM, CP, IR, MA, MP, PE, PS, SI
- Overlays for lines of business:
  - HIPAA
  - Military
  - Financial
  - ICS/SCADA

128

FIPS 200: Selecting Security Controls

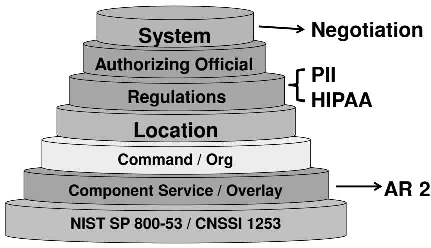
Task 2-2 › Select Security Controls

- Using SP 800-53
- Achieve Adequate Security
- Control selection based on FIPS 199 Impact Level:
  - For low-impact information systems, organizations must employ appropriate controls from low baseline of controls defined in NIST SP 800-53.
  - For moderate-impact information systems, moderate baseline.
  - For high-impact information systems, high baseline.

129

Tailoring Controls

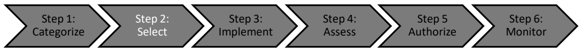
Task 2-2 › Select Security Controls



130

Task 2-3: Monitoring Strategy

Task 2-3	**Monitoring Strategy** • Configuration management and control processes • Security impact of proposed or actual changes • Assessment of selected controls • Security status reporting
Documents	System Security Plan
Roles	Information System Owner Common Control Provider
SDLC	Initiation (concept/requirements definition)



131

Monitored Control Selection

Task 2-3 › Monitoring Strategy

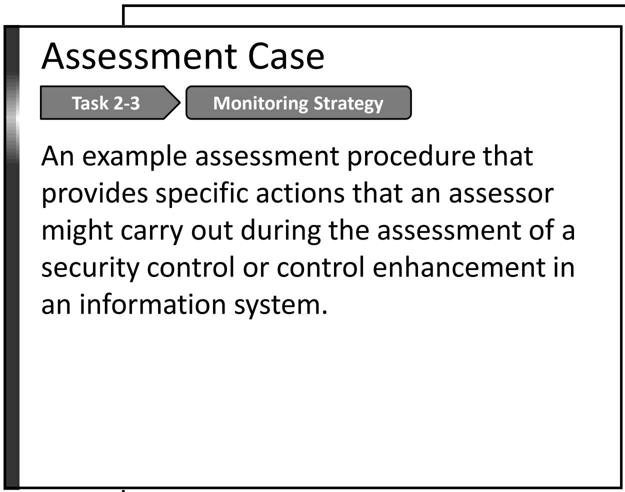
Which controls?

- Determined by the information system owner or common control provider
- Controls that are volatile, critical, or in the POAM

How often?

- Determination of trustworthiness of the common control provider
- Risk assessment
- Continues throughout life cycle

132

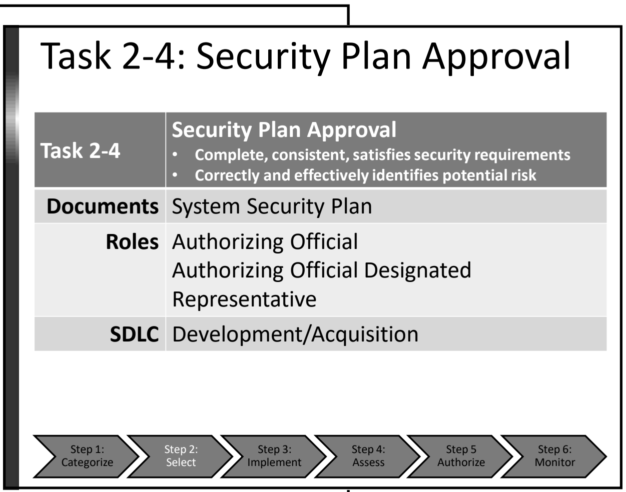


Assessment Case

Task 2-3 › Monitoring Strategy

An example assessment procedure that provides specific actions that an assessor might carry out during the assessment of a security control or control enhancement in an information system.

133

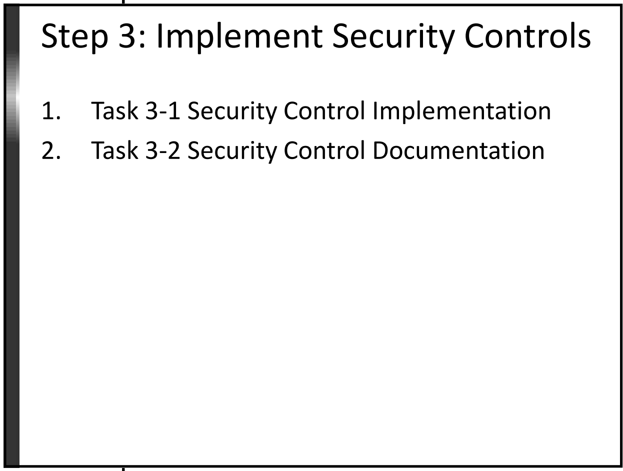


Task 2-4: Security Plan Approval

Task 2-4	**Security Plan Approval** • Complete, consistent, satisfies security requirements • Correctly and effectively identifies potential risk
Documents	System Security Plan
Roles	Authorizing Official Authorizing Official Designated Representative
SDLC	Development/Acquisition

Step 1: Categorize › Step 2: Select › Step 3: Implement › Step 4: Assess › Step 5 Authorize › Step 6: Monitor

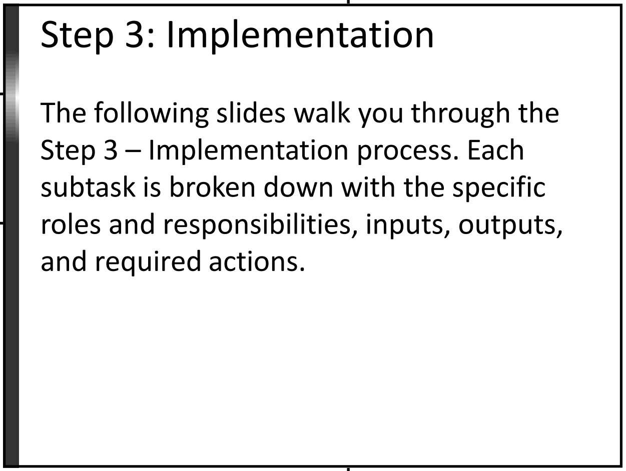
134



Step 3: Implement Security Controls

1. Task 3-1 Security Control Implementation
2. Task 3-2 Security Control Documentation

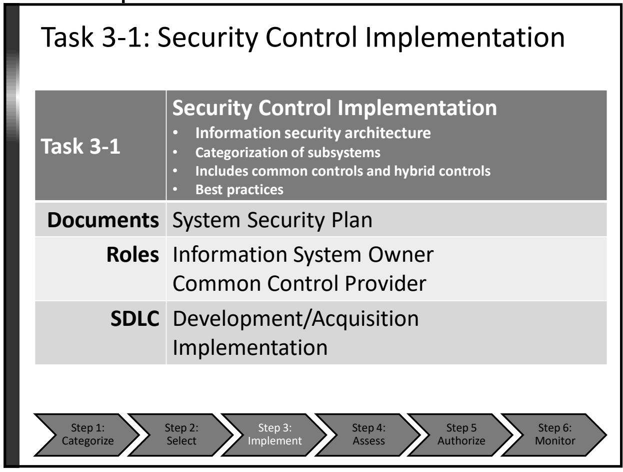
135



Step 3: Implementation

The following slides walk you through the Step 3 – Implementation process. Each subtask is broken down with the specific roles and responsibilities, inputs, outputs, and required actions.

136

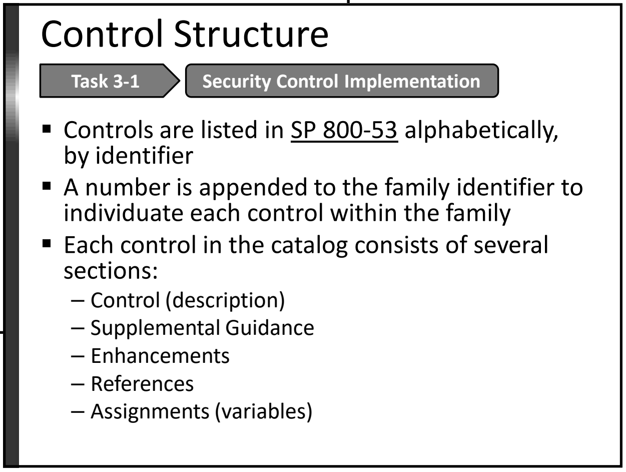


Task 3-1: Security Control Implementation

Task 3-1	**Security Control Implementation** • Information security architecture • Categorization of subsystems • Includes common controls and hybrid controls • Best practices
Documents	System Security Plan
Roles	Information System Owner Common Control Provider
SDLC	Development/Acquisition Implementation

Step 1: Categorize › Step 2: Select › Step 3: Implement › Step 4: Assess › Step 5 Authorize › Step 6: Monitor

137



Control Structure

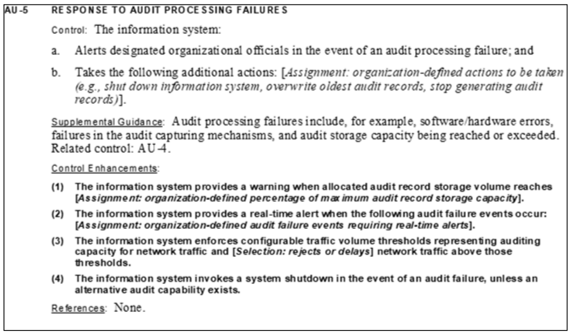
Task 3-1 › Security Control Implementation

- Controls are listed in SP 800-53 alphabetically, by identifier
- A number is appended to the family identifier to individuate each control within the family
- Each control in the catalog consists of several sections:
  - Control (description)
  - Supplemental Guidance
  - Enhancements
  - References
  - Assignments (variables)

138

Control Listing Example

Task 3-1 | Security Control Implementation



AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

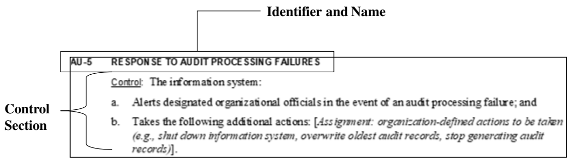
(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

Section: Control

Task 3-1 | Security Control Implementation

- Concise statement of specific security capability needed to protect particular aspect of organization or IS
- Describes security activities or actions to be performed


Identifier and Name
Control Section

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

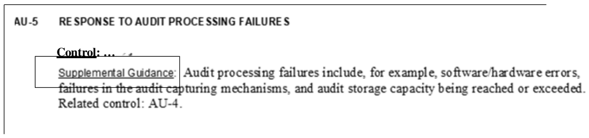
a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Section: Supplemental Guidance

Task 3-1 | Security Control Implementation

- Additional information related to specific security control
- Organizations apply supplemental guidance as appropriate



AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

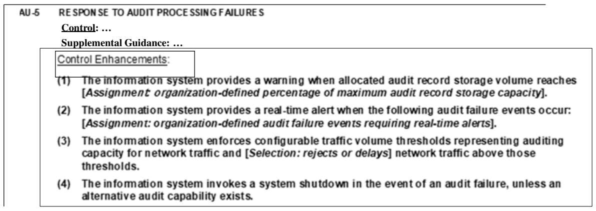
Control: …

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Section: Control Enhancements

Task 3-1 | Security Control Implementation

- Build in additional, but related, functionality to basic control, or Increase strength of basic control
- Provide greater protection needed due to potential impact of loss
- Numbered sequentially within each control; Designate selection by number
  - Example: See below. If the first three control enhancements are selected, the control designation becomes AU-5 (1) (2) (3)



AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: …

Supplemental Guidance: …

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

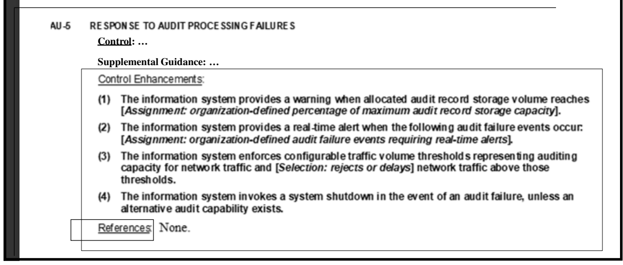
(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

Section: References

Task 3-1 | Security Control Implementation

- List any applicable federal laws, Executive Orders, directives, policies, standards, guidelines, etc.
- May also contain pertinent websites



AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: …

Supplemental Guidance: …

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

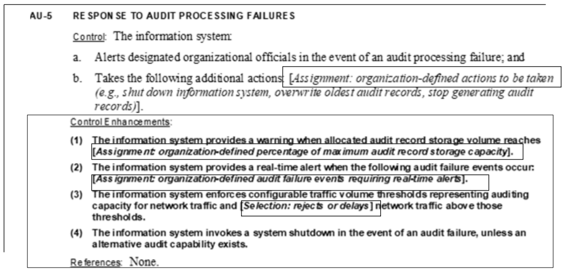
(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

Section: Assignments

Task 3-1 | Security Control Implementation

- Designates where organization establishes the specific value of certain parameters (variables)



AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

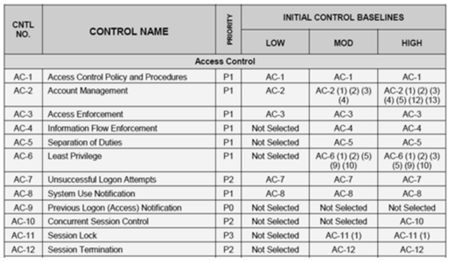
(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

SP 800-53 Table Structure

Task 3-1 | Security Control Implementation

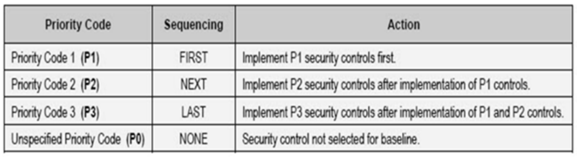


CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12

145

Prioritization Codes

Task 3-1 | Security Control Implementation



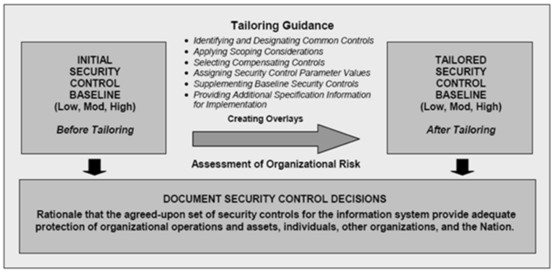
Priority Code	Sequencing	Action
Priority Code 1 (**P1**)	FIRST	Implement P1 security controls first.
Priority Code 2 (**P2**)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (**P3**)	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code (**P0**)	NONE	Security control not selected for baseline.

- Sequence of Installation only
- Does *not* relate to achievement of level of mitigation
- Remember, *not* used by DOD

146

Tailoring Controls

Task 3-1 | Security Control Implementation



INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)

Before Tailoring

Tailoring Guidance

- *Identifying and Designating Common Controls*
- *Applying Scoping Considerations*
- *Selecting Compensating Controls*
- *Assigning Security Control Parameter Values*
- *Supplementing Baseline Security Controls*
- *Providing Additional Specification Information for Implementation*

Creating Overlays

Assessment of Organizational Risk

TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)

After Tailoring

DOCUMENT SECURITY CONTROL DECISIONS

Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

FIGURE 4: SECURITY CONTROL SELECTION PROCESS

147

Tailoring Controls

Task 3-1 | Security Control Implementation

- 3 primary areas
  - Scoping Guidance
  - Compensating Controls
  - Organizational-defined parameter specifications
- Aligned with operational activities
- Aligned with operating environment

Note: Review Tailoring Pyramid from last chapter.

148

Scoping Guidance Areas

Task 3-1 | Security Control Implementation

- Common Control
- Security Objective
- System Component Allocation
- Technology
- Physical Infrastructure
- Policy/Regulatory
- Operational/Environmental
- Scalability
- Public Access

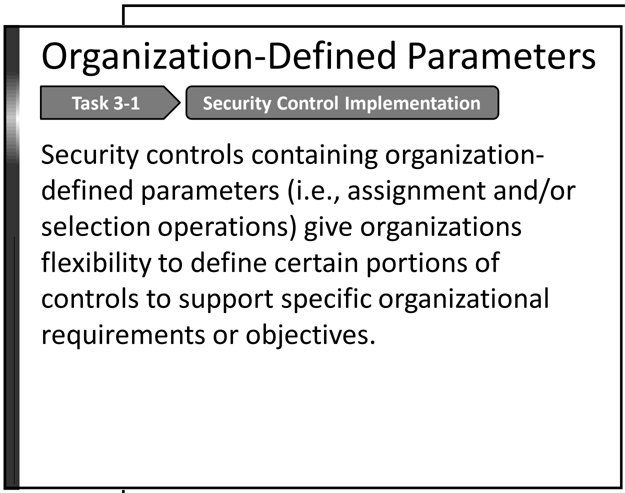
149

Scoping Considerations

Task 3-1 | Security Control Implementation

- Control Allocation and Placement Considerations
- Operational/Environmental–Related Considerations
  - Mobility
  - Single-User Systems and Operations
  - Data Connectivity and Bandwidth
  - Limited Functionality Systems or Components
  - Information and System Non-Persistence
  - Public Access
- Security Objective-Related Considerations
- Technology-Related Considerations
- Mission Requirements-Related Considerations

150

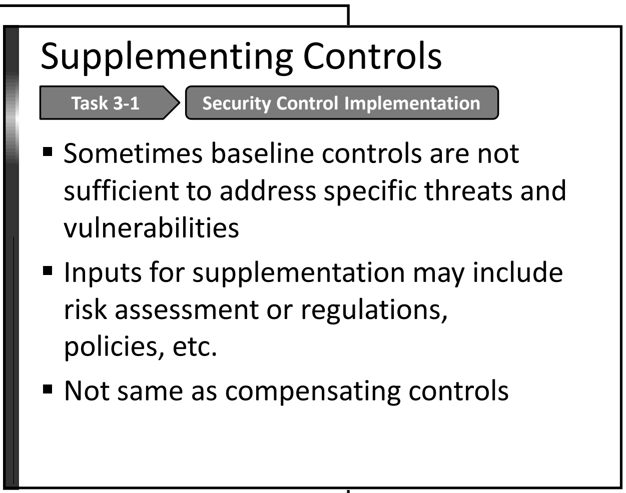


Organization-Defined Parameters

Task 3-1 | Security Control Implementation

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations flexibility to define certain portions of controls to support specific organizational requirements or objectives.

151

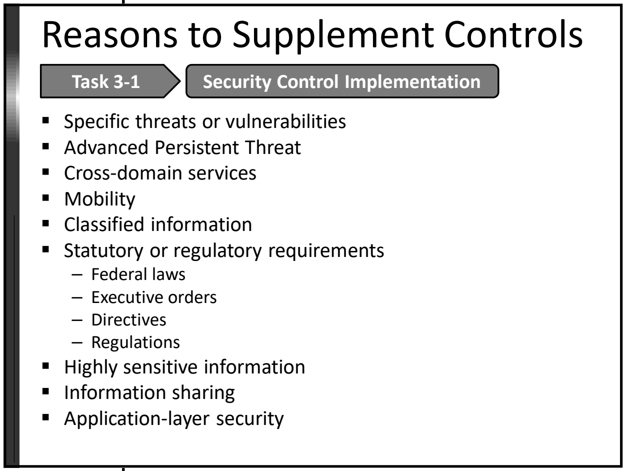


Supplementing Controls

Task 3-1 | Security Control Implementation

- Sometimes baseline controls are not sufficient to address specific threats and vulnerabilities
- Inputs for supplementation may include risk assessment or regulations, policies, etc.
- Not same as compensating controls

152

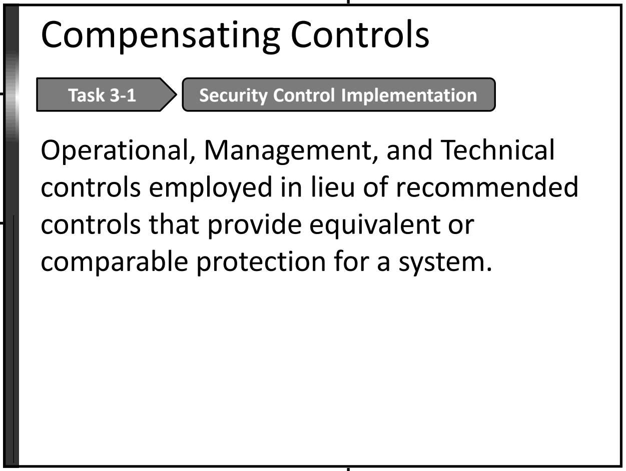


Reasons to Supplement Controls

Task 3-1 | Security Control Implementation

- Specific threats or vulnerabilities
- Advanced Persistent Threat
- Cross-domain services
- Mobility
- Classified information
- Statutory or regulatory requirements
  - Federal laws
  - Executive orders
  - Directives
  - Regulations
- Highly sensitive information
- Information sharing
- Application-layer security

153

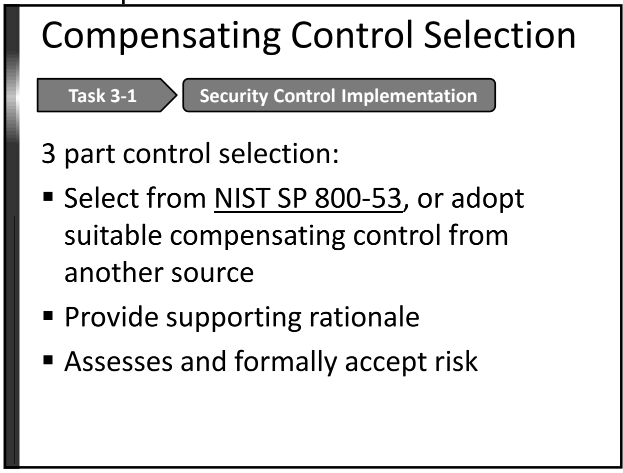


Compensating Controls

Task 3-1 | Security Control Implementation

Operational, Management, and Technical controls employed in lieu of recommended controls that provide equivalent or comparable protection for a system.

154



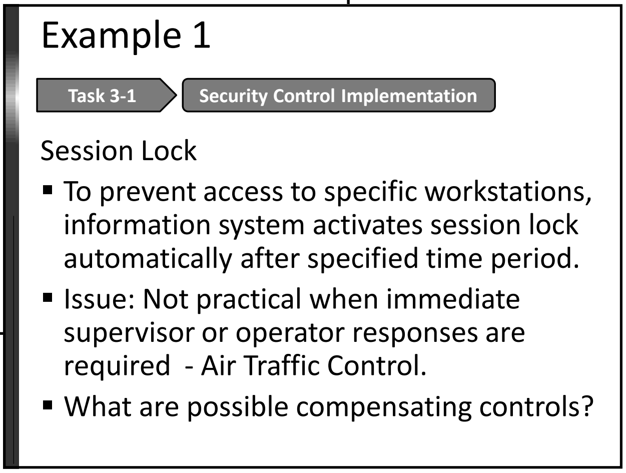
Compensating Control Selection

Task 3-1 | Security Control Implementation

3 part control selection:

- Select from NIST SP 800-53, or adopt suitable compensating control from another source
- Provide supporting rationale
- Assesses and formally accept risk

155



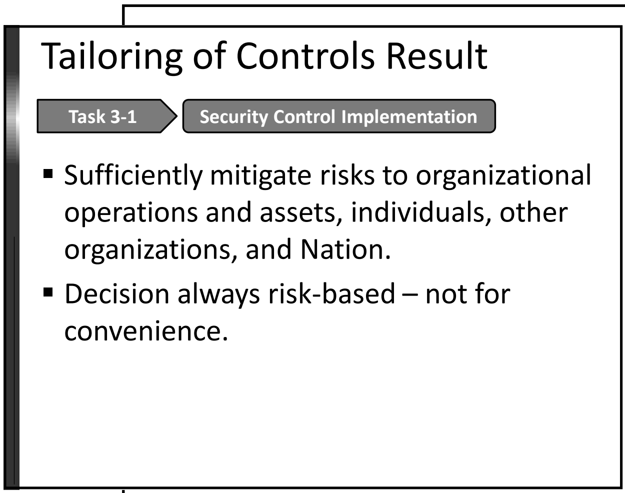
Example 1

Task 3-1 | Security Control Implementation

Session Lock

- To prevent access to specific workstations, information system activates session lock automatically after specified time period.
- Issue: Not practical when immediate supervisor or operator responses are required - Air Traffic Control.
- What are possible compensating controls?

156

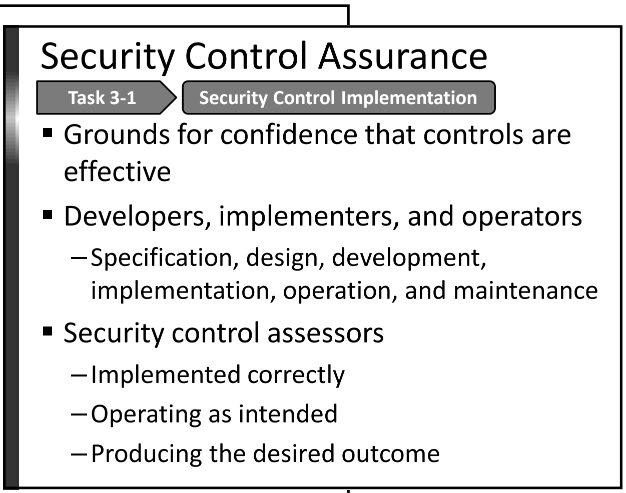


Tailoring of Controls Result

Task 3-1 | Security Control Implementation

- Sufficiently mitigate risks to organizational operations and assets, individuals, other organizations, and Nation.
- Decision always risk-based – not for convenience.

157

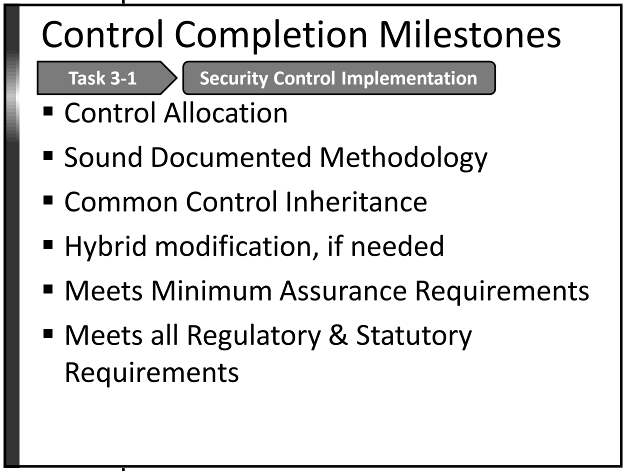


Security Control Assurance

Task 3-1 | Security Control Implementation

- Grounds for confidence that controls are effective
- Developers, implementers, and operators
  - Specification, design, development, implementation, operation, and maintenance
- Security control assessors
  - Implemented correctly
  - Operating as intended
  - Producing the desired outcome

158

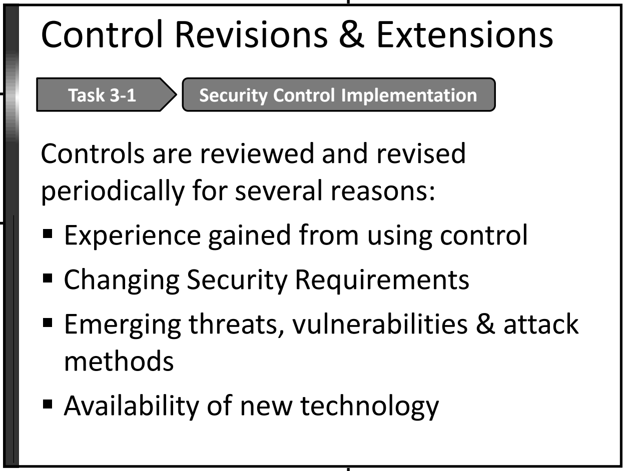


Control Completion Milestones

Task 3-1 | Security Control Implementation

- Control Allocation
- Sound Documented Methodology
- Common Control Inheritance
- Hybrid modification, if needed
- Meets Minimum Assurance Requirements
- Meets all Regulatory & Statutory Requirements

159



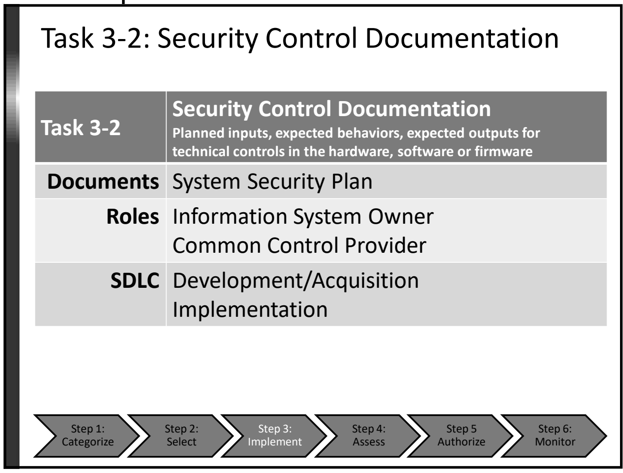
Control Revisions & Extensions

Task 3-1 | Security Control Implementation

Controls are reviewed and revised periodically for several reasons:

- Experience gained from using control
- Changing Security Requirements
- Emerging threats, vulnerabilities & attack methods
- Availability of new technology

160

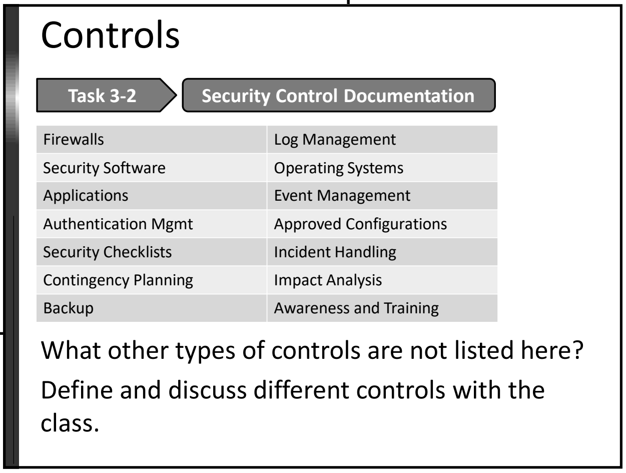


Task 3-2: Security Control Documentation

Task 3-2	**Security Control Documentation** Planned inputs, expected behaviors, expected outputs for technical controls in the hardware, software or firmware
Documents	System Security Plan
Roles	Information System Owner Common Control Provider
SDLC	Development/Acquisition Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

161



Controls

Task 3-2 | Security Control Documentation

Firewalls	Log Management
Security Software	Operating Systems
Applications	Event Management
Authentication Mgmt	Approved Configurations
Security Checklists	Incident Handling
Contingency Planning	Impact Analysis
Backup	Awareness and Training

What other types of controls are not listed here?

Define and discuss different controls with the class.

162

Security Controls Documentation

Task 3-2 › Security Control Documentation

- Document the control implementation in SSP:
  - Planned inputs
  - Expected Behavior
  - Expected Outputs
- Functional Description
- Traceability Matrix to Requirements
- Platform Dependencies
- Responsible Person/CCP

163

Developer & Stakeholder Activities

Task 3-2 › Security Control Documentation

Developer:

- Provide system architecture and software design
- Identify all necessary network connections
- Provide assurance of integrity of all integrated components

Stakeholder:

- Conduct initial certification analysis
- Forward design revisions and certification analyses to developer throughout system development
- Conduct system test readiness review

164

Step 4: Key References

- NIST Special Publications:
  - 800-30 Rev1: Risk Assessment
  - 800-53A Rev4: Control Assessment
  - 800-115: Technical Assessment

165

Step 4: Assess Security Controls

1. Task 4-1 Assessment Preparation
2. Task 4-2 Security Control Assessment
3. Task 4-3 Security Assessment Report
4. Task 4-4 Remediation Actions

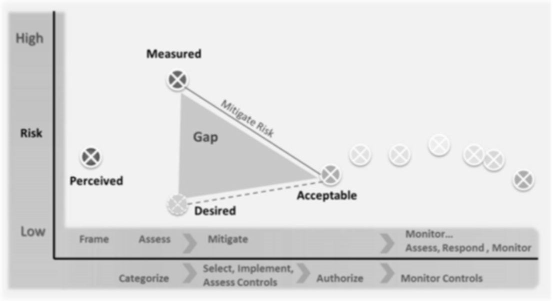
166

6 Key Areas for Assessment

- Prepare for security control assessment
- Establish security control assessment plan
- Determine security control effectiveness
- Develop initial security assessment report
- Perform initial remediation actions
- Develop final security assessment report and addendum

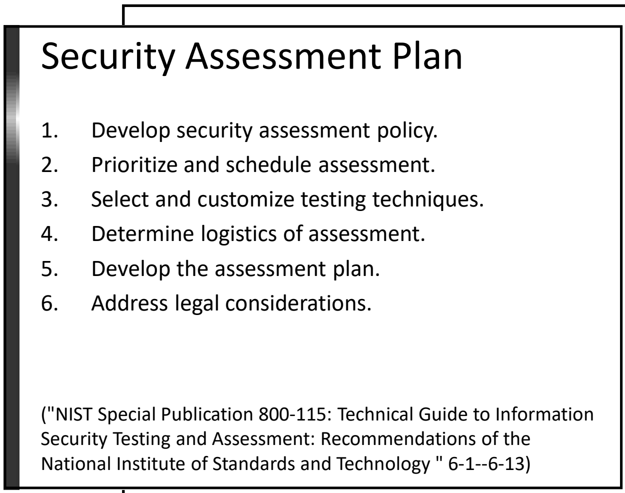
167

Why Assess? – Gap Analysis



(From FITSI.ORG/FITSP-M)

168

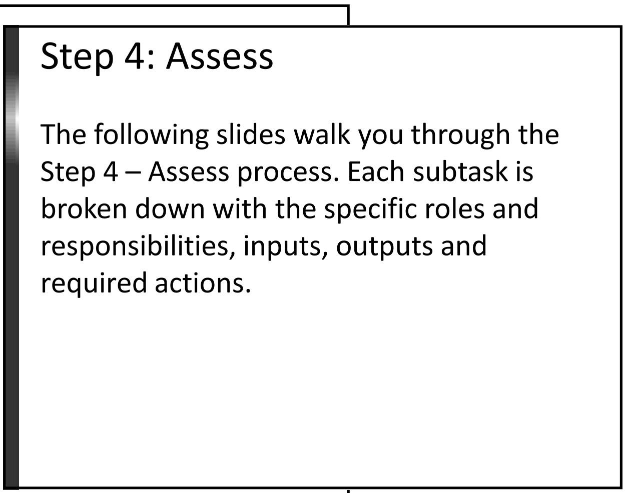


Security Assessment Plan

1. Develop security assessment policy.
2. Prioritize and schedule assessment.
3. Select and customize testing techniques.
4. Determine logistics of assessment.
5. Develop the assessment plan.
6. Address legal considerations.

("NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology " 6-1--6-13)

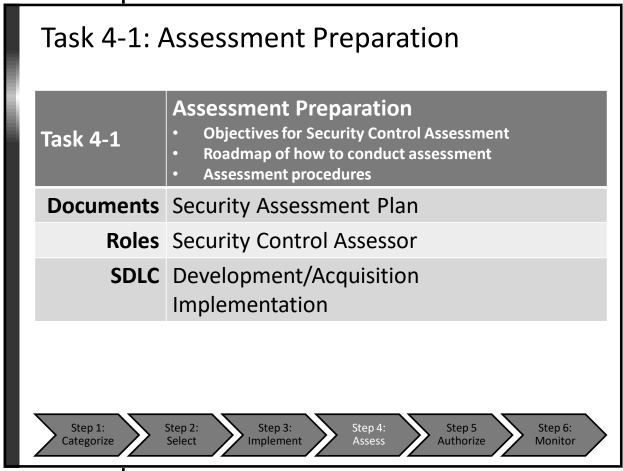
169



Step 4: Assess

The following slides walk you through the Step 4 – Assess process. Each subtask is broken down with the specific roles and responsibilities, inputs, outputs and required actions.

170

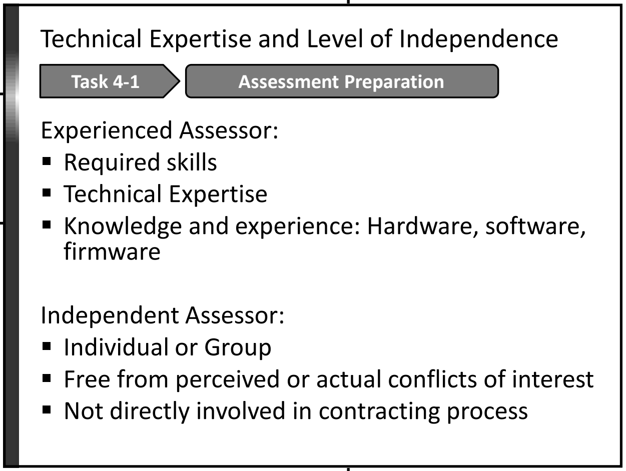


Task 4-1: Assessment Preparation

Task 4-1	**Assessment Preparation** • **Objectives for Security Control Assessment** • **Roadmap of how to conduct assessment** • **Assessment procedures**
Documents	Security Assessment Plan
Roles	Security Control Assessor
SDLC	Development/Acquisition Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

171



Technical Expertise and Level of Independence

Task 4-1 → Assessment Preparation

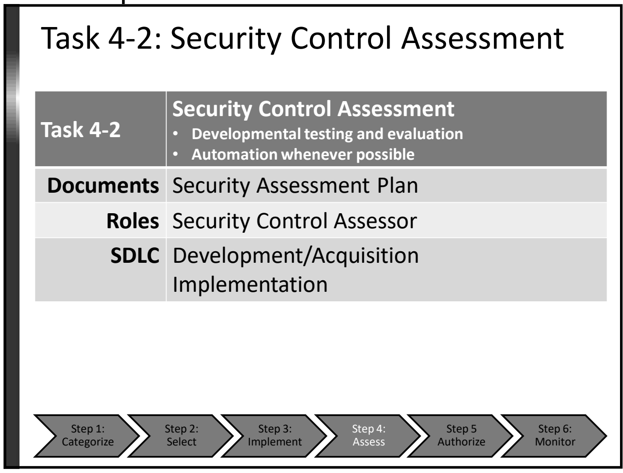
Experienced Assessor:

- Required skills
- Technical Expertise
- Knowledge and experience: Hardware, software, firmware

Independent Assessor:

- Individual or Group
- Free from perceived or actual conflicts of interest
- Not directly involved in contracting process

172

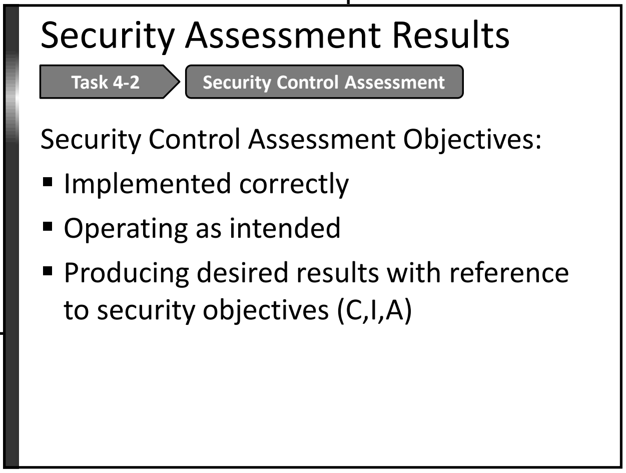


Task 4-2: Security Control Assessment

Task 4-2	**Security Control Assessment** • **Developmental testing and evaluation** • **Automation whenever possible**
Documents	Security Assessment Plan
Roles	Security Control Assessor
SDLC	Development/Acquisition Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

173



Security Assessment Results

Task 4-2 → Security Control Assessment

Security Control Assessment Objectives:

- Implemented correctly
- Operating as intended
- Producing desired results with reference to security objectives (C,I,A)

174

Original Assessment Methods

Task 4-2 | Security Control Assessment

Assessment procedure steps will include the appropriate evaluation method(s) from the following list:

- Test (T)
- Observation (O)
- Document Review (D)
- Interview (I)

175

Methods of Security Assessment

Assessment: Determining how effectively an entity being assessed meets specific security objectives.

Testing

Examination

Interviewing

176

NIST Methods for Assessment

Task 4-2 | Security Control Assessment

- **Examine**
  - Observation & Review
- **Interview**
- **Test**

Attributes to look for:

- Depth (Basic, Focused, Comprehensive)
- Coverage (Basic, Focused, Comprehensive)
- Determined by Assurance Requirements
- Defined by Organization

177

Assessment Tasks

Task 4-2 | Security Control Assessment

- Ensure proper policies in place
- Ensure all previous RMF Steps completed
- Ensure all Common Controls in place and implemented
- Collect and evaluate system artifacts
- Assessment testing:
  - Vulnerability scanning
  - Log review
  - Penetration testing
  - Configuration checklist review

178

Strategies for Conducting Assessments

Task 4-2 | Security Control Assessment

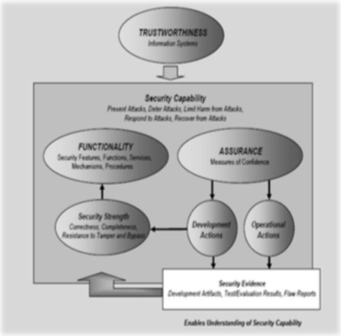
- Maximize use of common controls
- Share assessment results
- Develop organization-wide procedures
- Provide organization-wide tools, templates, techniques

179

Building an Effective Assurance Case

Task 4-2 | Security Control Assessment

- Compiling and presenting evidence
- Basis for determining effectiveness of controls
- Product assessments
- Systems assessment
- Risk determination


TRUSTWORTHINESS
Information Systems
Security Capability
Prevent Attacks, Deter Attacks, Limit Harm from Attacks, Respond to Attacks, Recover from Attacks
FUNCTIONALITY
Security Features, Functions, Services, Mechanisms, Procedures
ASSURANCE
Measures of Confidence
Security Strength
Correctness, Completeness, Resistance to Tamper and Bypass
Development Actions
Operational Actions
Security Evidence
Development Artifacts, Test/Evaluation Results, Flaw Reports
Enables Understanding of Security Capability

180

Assessment Procedures

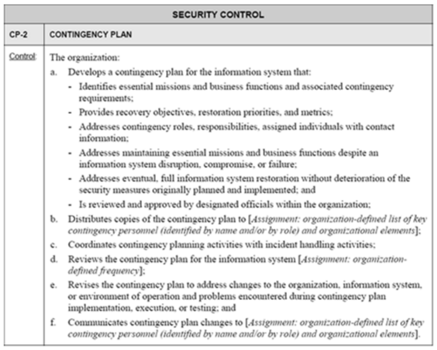
Task 4-2 | Security Control Assessment

- Assessment Objectives
- Determination Statements
- Assessment Methods
- Assessment Objects
- Assessment Findings

181

Example: Control Definition

Task 4-2 | Security Control Assessment

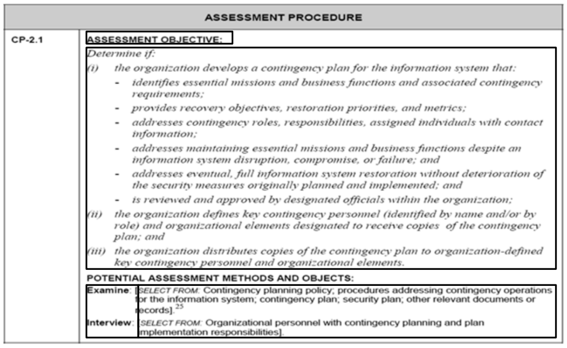


SECURITY CONTROL	
CP-2	CONTINGENCY PLAN
Control:	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

182

Objective Determination Statement

Task 4-2 | Security Control Assessment

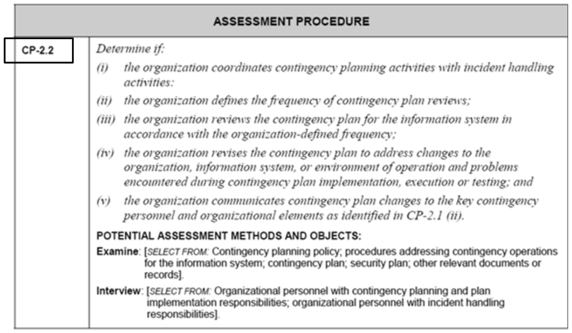


ASSESSMENT PROCEDURE	
CP-2.1	ASSESSMENT OBJECTIVE: *Determine if:* *(i) the organization develops a contingency plan for the information system that:* *- identifies essential missions and business functions and associated contingency requirements;* *- provides recovery objectives, restoration priorities, and metrics;* *- addresses contingency roles, responsibilities, assigned individuals with contact information;* *- addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and* *- addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and* *- is reviewed and approved by designated officials within the organization;* *(ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan; and* *(iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records].[25] **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

183

Subsequent Objectives

Task 4-2 | Security Control Assessment



ASSESSMENT PROCEDURE	
CP-2.2	*Determine if:* *(i) the organization coordinates contingency planning activities with incident handling activities:* *(ii) the organization defines the frequency of contingency plan reviews;* *(iii) the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;* *(iv) the organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing; and* *(v) the organization communicates contingency plan changes to the key contingency personnel and organizational elements as identified in CP-2.1 (ii).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities].

184

Assessment Objects

Task 4-2 | Security Control Assessment

- Specifications (Artifacts)
- Mechanisms (Components of an IS)
- Activities (Actions)
- Individuals

185

Benefits of Repeatable & Documented Methods

Task 4-2 | Security Control Assessment

- Provide consistency and structure
- Minimize testing risks
- Expedite transition of new staff
- Address resource constraints
- Reuse resources
- Decrease time required
- Cost reduction

186

System & Network Assessment Methods

Task 4-2 Security Control Assessment

- Log reviews
- File integrity checkers
- Penetration testing
- Vulnerability scanning
- Social engineering
- Wireless scanning
- Network scanning and discovery
- Prior Assessment Reports

187

Technical Assessment Techniques 1

Task 4-2 Security Control Assessment

- Review techniques:
  - Documentation review
  - Log review
  - Ruleset review
  - System configuration review
  - Network sniffing
  - File integrity checkers
- Target ID and analysis techniques:
  - Network discovery
  - Network port and services identification
  - Vulnerability scanning
  - Wireless scans

188

Technical Assessment Techniques 2

Task 4-2 Security Control Assessment

- Vulnerability tools and techniques:
  - Network scanning
  - Vulnerability scanners
  - War dialing
  - War driving
- Target vulnerability validation techniques:
  - Password cracking
  - Penetration testing
  - Social engineering

189

Task 4-3: Security Assessment Report

Task 4-3	**Security Assessment Report** • Issues and findings • Recommendations for correcting weaknesses and inefficiencies
Documents	Security Assessment Report
Roles	Security Control Assessor
SDLC	Development/Acquisition Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

190

Task 4-4: Remediation Actions

Task 4-4	**Remediation Actions** • Review and prioritization of findings • Remediation actions • Reassessment of risk
Documents	Security Assessment Report
Roles	Information System Owner Common Control Provider Security Control Assessor
SDLC	Development/Acquisition Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

191

Chapter 9:
Step 5: Authorize

Upon completion of this chapter, you will be able to:

- Support the creation and completion of the plan of action and milestones (POA&M) in accordance with your RMF role.
- Describe the contents of the security authorization package.
- Authorize or support the authorization of the information system.
- State the level of acceptable risk for your information system.
- Adhere to the correct procedures when a system is authorized to operate, given interim authorization, or not authorized to operate .

CAP Exam Prep

- The authorization step of the RMF process is the focus of many CAP exam questions.

192

Building an Effective Assurance Case

- Compiling and presenting evidence
- Basis for determining effectiveness of controls
- Product assessments
- Systems assessment
- Risk determination

193

Step 5: Authorize Information System

1. Task 5-1 Plan of Action and Milestones
2. Task 5-2 Security Authorization Package
3. Task 5-3 Risk Determination
4. Task 5-4 Risk Acceptance

194

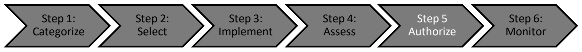
Step 5: Authorize

The following slides walk you through the Step 5 – Authorize process. Each subtask is broken down with the specific roles and responsibilities, inputs, outputs and required actions.

195

Task 5-1: Plan of Action and Milestones

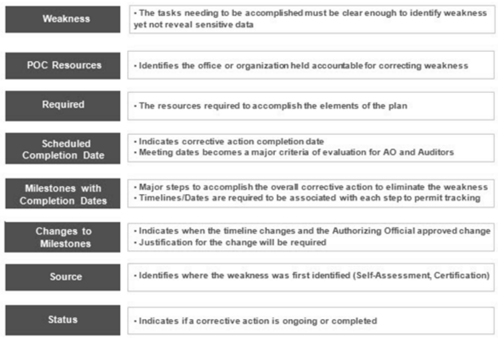
Task 5-1	**Plan of Action and Milestones** • Describes remediation tasks • Allocates resources to tasks • Sets milestones and schedule for task completion
Documents	Plan of Action and Milestones
Roles	Information System Owner Common Control Provider
SDLC	Implementation


Step 1: Categorize
Step 2: Select
Step 3: Implement
Step 4: Assess
Step 5 Authorize
Step 6: Monitor

196

POA&M Layout

Task 5-1 Plan of Action and Milestones



Weakness	• The tasks needing to be accomplished must be clear enough to identify weakness yet not reveal sensitive data
POC Resources	• Identifies the office or organization held accountable for correcting weakness
Required	• The resources required to accomplish the elements of the plan
Scheduled Completion Date	• Indicates corrective action completion date • Meeting dates becomes a major criteria of evaluation for AO and Auditors
Milestones with Completion Dates	• Major steps to accomplish the overall corrective action to eliminate the weakness • Timelines/Dates are required to be associated with each step to permit tracking
Changes to Milestones	• Indicates when the timeline changes and the Authorizing Official approved change • Justification for the change will be required
Source	• Identifies where the weakness was first identified (Self-Assessment, Certification)
Status	• Indicates if a corrective action is ongoing or completed

197

POA&M Fields

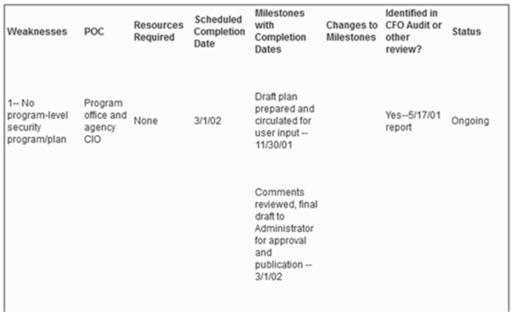
Task 5-1 Plan of Action and Milestones

- Type of weaknesses
- Office or organization responsible for correcting weaknesses
- Amount of money needed to correct weaknesses
- Scheduled completion date for weaknesses
- Key milestones with completion dates
- Milestone changes
- Source of weaknesses
- Status

198

Sample POA&M

Task 5-1 | Plan of Action and Milestones



Weaknesses	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Status
1-- No program-level security program/plan	Program office and agency CIO	None	3/1/02	Draft plan prepared and circulated for user input -- 11/30/01		Yes--5/17/01 report	Ongoing
				Comments reviewed, final draft to Administrator for approval and publication -- 3/1/02			

199

Task 5-2: Security Authorization Package

Task 5-2	**Security Authorization Package** • Protected by federal and organizational policies • Strongly encouraged to use automated support tools to prepare and manage
Documents	System Security Plan Security Assessment Report Plan of Action and Milestones
Roles	Information System Owner Common Control Provider
SDLC	Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

200

Security Authorization Package: What's Inside?

Task 5-2 | Security Authorization Package

System Security Plan — An overview of security requirements, description of agree-upon security controls, and other supporting security-related documents

Security Assessment Report — Security control assessment results and recommended corrective actions for control weaknesses or deficiencies.

Plan of Action and Milestones — Measures planned to correct weaknesses or deficiencies and to reduce or eliminate know vulnerabilities

201

Task 5-3: Risk Determination

Task 5-3	**Risk Determination** • Current security state of the system • Recommendations for addressing residual risks • Threats, vulnerabilities, potential impacts
Documents	System Security Plan Security Assessment Report Plan of Action and Milestones
Roles	Authorizing Official Designated Representative
SDLC	Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

202

Risk Management Strategy

Task 5-3 | Risk Determination

- How is risk identified?
- How is risk evaluated?
- How is risk addressed?
- What is risk accepted?
- How is risk monitored?

203

Task 5-4: Risk Acceptance

Task 5-4	**Risk Acceptance** • Authorization decision • Terms and conditions for authorization • Authorization termination date
Documents	Authorizing Decision Document
Roles	Authorizing Official (only)
SDLC	Implementation

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

204

Authorization to Operate (ATO)

Task 5-4 | Risk Acceptance

205

Denial of Authorization to Operate (DATO)

Task 5-4 | Risk Acceptance

206

Authorization Decision Document

Task 5-4 | Risk Acceptance

- Authorization decision
- Terms and conditions for authorization
- Authorization termination date
- Risk executive (function) input (if provided)

207

Authorization Decision Document

Task 5-4 | Risk Acceptance

- Security Accreditation Decision Letter
  - Security accreditation decision
    - Supporting rationale for accreditation decision
  - Terms and conditions for authorization
  - Authorization termination date
- Prepared by the Authorizing Official's Designated Representative

208

Continuous Monitoring

- Near real-time risk management
- Ongoing updates to Security plan, SAR, and POAM
- Reduces level of effort needed for reauthorization
- Scaled with information system's impact level

209

Step 6: Monitor

The following slides walk you through the Step 6 – Monitor process.

Each subtask is broken down with the specific roles and responsibilities, inputs, outputs and required actions.

210

Task 6-1: Information System & Environment Changes

Task 6-1	**Information System & Environment Changes** • Conduct impact analysis • Corrective actions initiated • Appropriate documents revised and updated
Documents	System Security Plan Security Assessment Report Plan of Action and Milestones
Roles	Information System Owner Common Control Provider
SDLC	Operation/Maintenance

Step 1: Categorize
Step 2: Select
Step 3: Implement
Step 4: Assess
Step 5 Authorize
Step 6: Monitor

211

Configuration Management Process

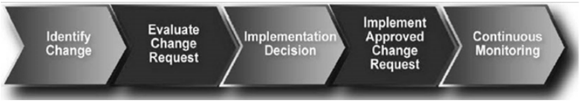
Security Impact Analysis of Change Requests

Task 6-1 › Information System & Environment Changes

- NIST SP 800-128
- Security-focused configuration management
- Every CR needs SIA = Security Impact Analysis prior to CCB approval of proposed change
- In DOD, this activity is currently falling on the ISSM in conjunction with system ISSO

212

System Configuration Management



- Control CA-7
- SP 800-128
- Security Configuration Mgmt first step for Monitoring System Status

213

Configuration Management Process

Patch and Vulnerability Management

Task 6-1 › Information System & Environment Changes

- Proactively prevent exploitation of vulnerabilities
- Reduce time and money spent on vulnerabilities
- Reduce, eliminate or manage exploitation
- Additional code developed to address known vulnerabilities in software
- Enable additional functionality or address security flaws
- SP 800-40 – PVM Program

214

Configuration Management Process

Security Content Automation Protocol (SCAP)

Task 6-1 › Information System & Environment Changes

A suite of specifications for organizing and expressing security-related information in standardized ways, as well as related reference data, such as identifiers for software flaws and security configuration issues.

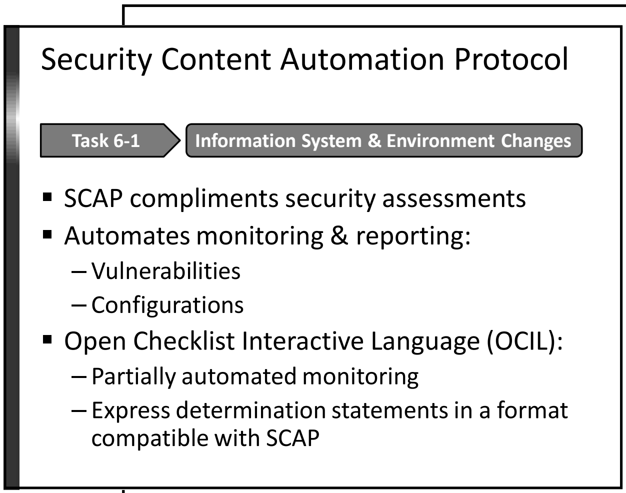
215

Automation and Reference Data Sources

Task 6-1 › Information System & Environment Changes

- Security Content Automation Protocol (SCAP)
  - What can be automated with SCAP
  - How to implement SCAP
  - Partially automated controls
- Reference data sources
  - National vulnerability database (NVD)
  - Security configuration checklists

216

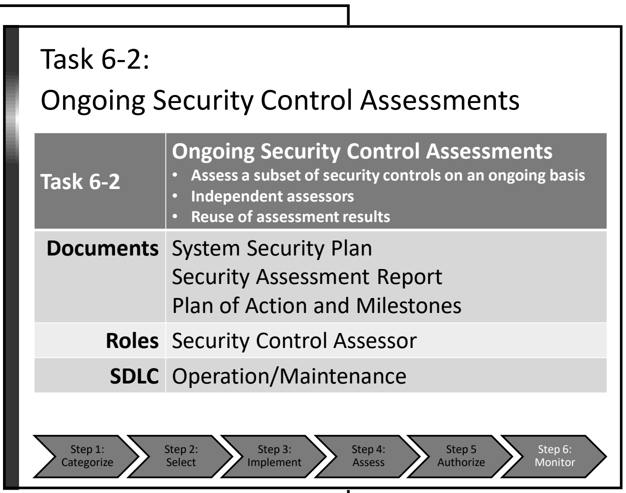


Security Content Automation Protocol

Task 6-1 → Information System & Environment Changes

- SCAP compliments security assessments
- Automates monitoring & reporting:
  - Vulnerabilities
  - Configurations
- Open Checklist Interactive Language (OCIL):
  - Partially automated monitoring
  - Express determination statements in a format compatible with SCAP

217

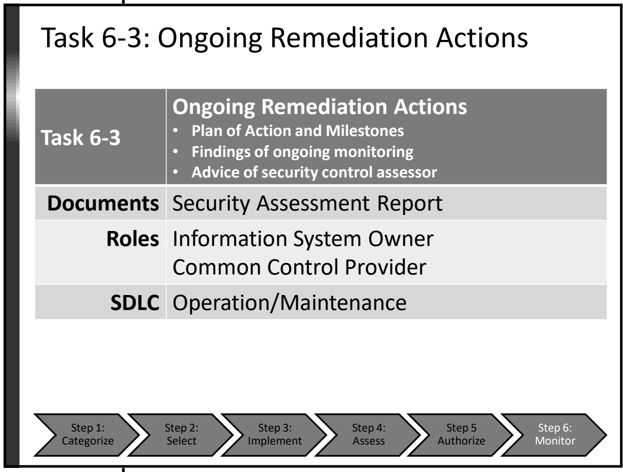


Task 6-2:
Ongoing Security Control Assessments

Task 6-2	**Ongoing Security Control Assessments** • Assess a subset of security controls on an ongoing basis • Independent assessors • Reuse of assessment results
Documents	System Security Plan Security Assessment Report Plan of Action and Milestones
Roles	Security Control Assessor
SDLC	Operation/Maintenance

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

218

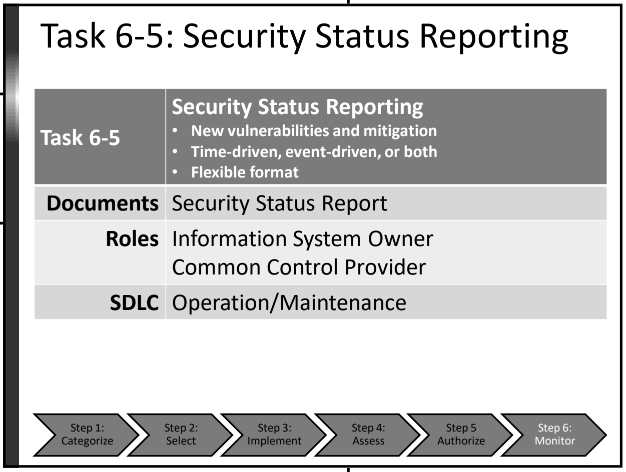


Task 6-3: Ongoing Remediation Actions

Task 6-3	**Ongoing Remediation Actions** • Plan of Action and Milestones • Findings of ongoing monitoring • Advice of security control assessor
Documents	Security Assessment Report
Roles	Information System Owner Common Control Provider
SDLC	Operation/Maintenance

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

219

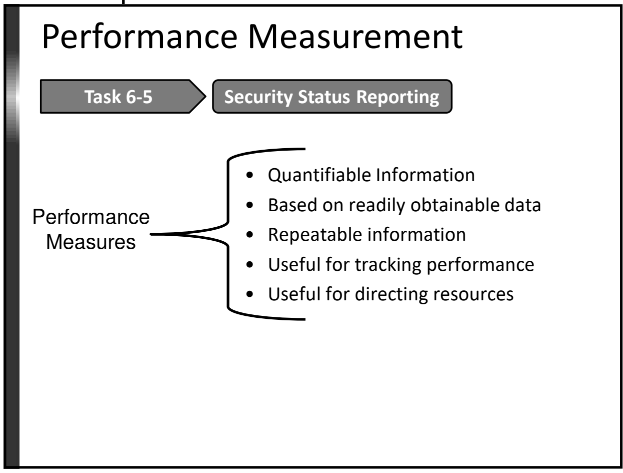


Task 6-5: Security Status Reporting

Task 6-5	**Security Status Reporting** • New vulnerabilities and mitigation • Time-driven, event-driven, or both • Flexible format
Documents	Security Status Report
Roles	Information System Owner Common Control Provider
SDLC	Operation/Maintenance

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

220



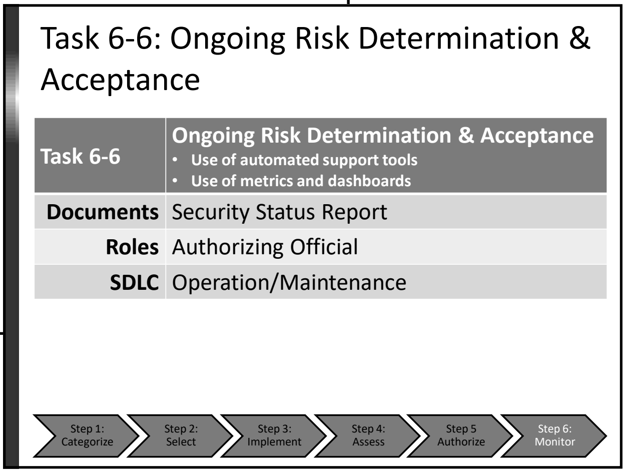
Performance Measurement

Task 6-5 → Security Status Reporting

Performance Measures

- Quantifiable Information
- Based on readily obtainable data
- Repeatable information
- Useful for tracking performance
- Useful for directing resources

221

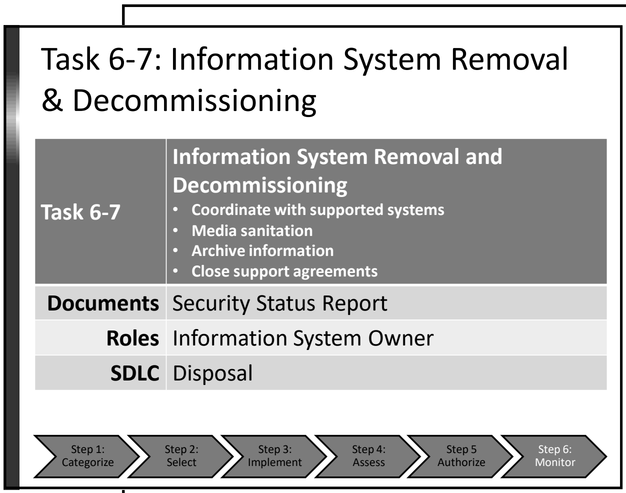


Task 6-6: Ongoing Risk Determination & Acceptance

Task 6-6	**Ongoing Risk Determination & Acceptance** • Use of automated support tools • Use of metrics and dashboards
Documents	Security Status Report
Roles	Authorizing Official
SDLC	Operation/Maintenance

Step 1: Categorize → Step 2: Select → Step 3: Implement → Step 4: Assess → Step 5 Authorize → Step 6: Monitor

222

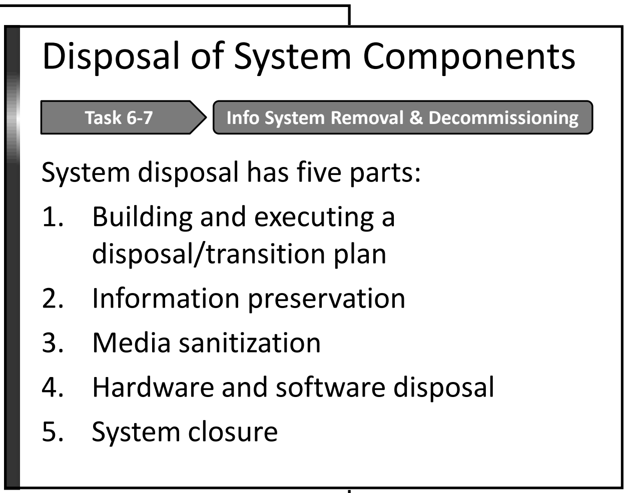


Task 6-7: Information System Removal & Decommissioning

Task 6-7	**Information System Removal and Decommissioning** • Coordinate with supported systems • Media sanitation • Archive information • Close support agreements
Documents	Security Status Report
Roles	Information System Owner
SDLC	Disposal

Step 1: Categorize
Step 2: Select
Step 3: Implement
Step 4: Assess
Step 5 Authorize
Step 6: Monitor

223



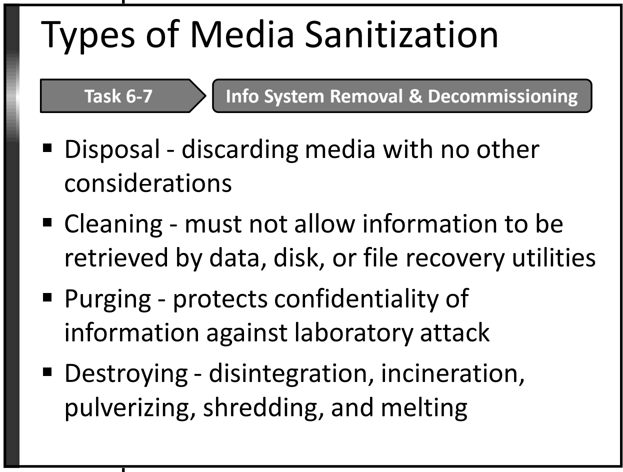
Disposal of System Components

Task 6-7 | Info System Removal & Decommissioning

System disposal has five parts:

1. Building and executing a disposal/transition plan
2. Information preservation
3. Media sanitization
4. Hardware and software disposal
5. System closure

224



Types of Media Sanitization

Task 6-7 | Info System Removal & Decommissioning

- Disposal - discarding media with no other considerations
- Cleaning - must not allow information to be retrieved by data, disk, or file recovery utilities
- Purging - protects confidentiality of information against laboratory attack
- Destroying - disintegration, incineration, pulverizing, shredding, and melting

225