LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

# The Department of Health and Human Services
# Information Security for Managers

Fiscal Year 2016

# Information Security for Managers


- Introduction
- Information Security Overview
- Enterprise Performance Life Cycle
- Enterprise Performance Life Cycle and the Risk Management Framework
  - Categorize the System and Select Controls
  - Implement and Assess the Controls
  - Monitor the Controls and System Disposal
- Summary
- Appendix

## Introduction

# Welcome to Information Security for Managers

As a Manager at the Department of Health and Human Services (HHS), you play a vital role in safeguarding HHS systems and information assets. This course will address a risk-based approach to enterprise-wide information security program management and provide an overview of your role in implementing and managing information systems.

References to HHS information security policies, standards, and guidance are provided for various course topics. Refer to your Operating Division's (OpDiv) security policies and procedures, in most cases they will be more specific than Department policy.

## Introduction

# Objectives

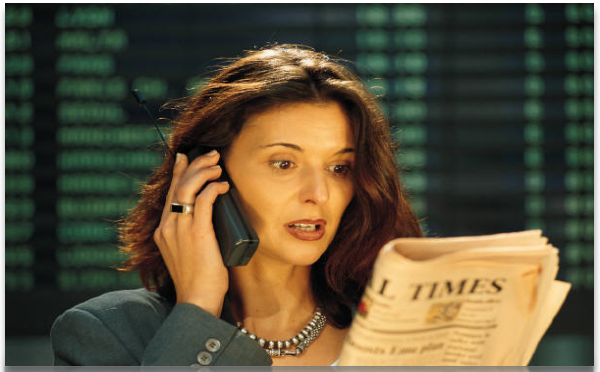
At the end of this course you will be able to:

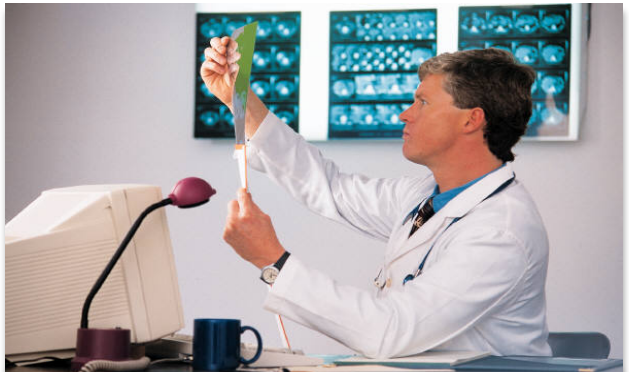
- ❑ Understand your role and responsibilities to protect information security as an HHS manager.
- ❑ Define the basic components of an information security program.
- ❑ Understand the Enterprise Performance Life Cycle (EPLC) and the Risk Management Framework (RMF) and how they relate to the development of information technology (IT) systems.
- ❑ Identify where to locate HHS policies, procedures, and guidance for developing, implementing, and managing information systems from beginning to end.

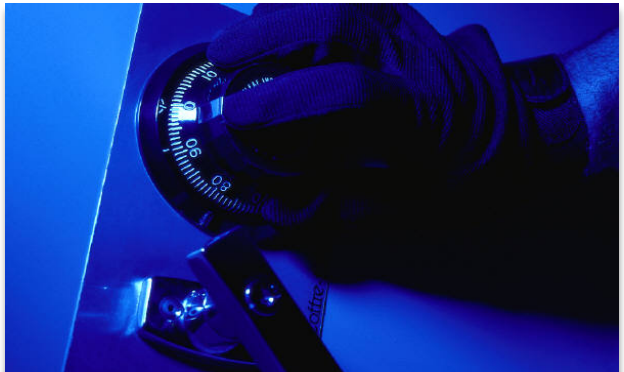
## Introduction

# What happens if….

- A story appears in the national news about HHS data being stolen or disclosed to unauthorized personnel?
- The public loses confidence in HHS because of a security breach involving personal data?
- Criminals hack into HHS networks and steal information, threatening the privacy and financial security for millions of people?



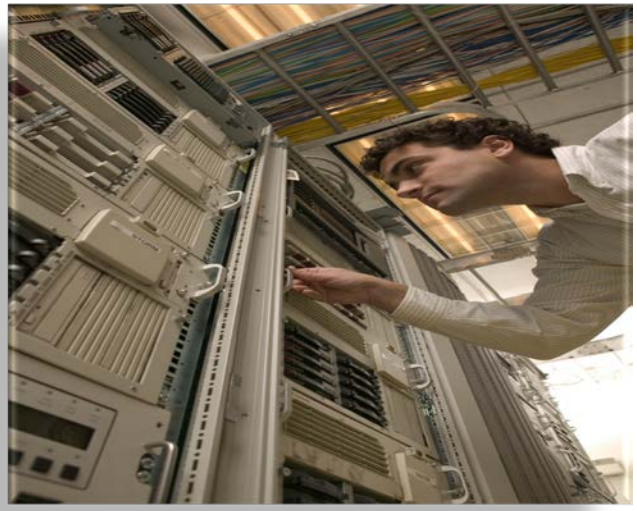




## Introduction

# Why is Information Security Important?

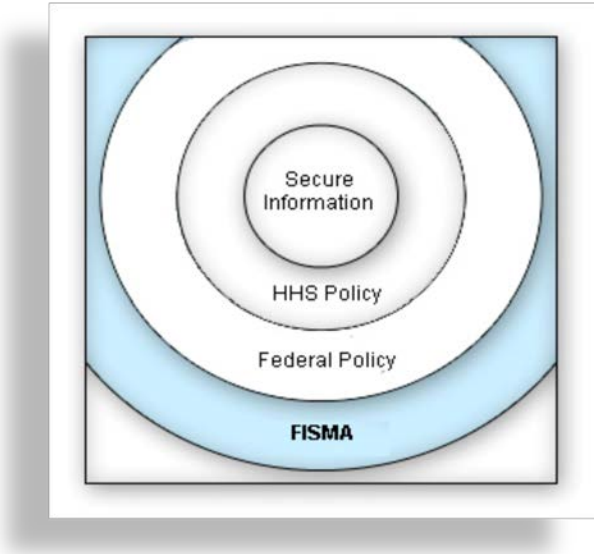
- The American people depend on HHS to keep sensitive information appropriately confidential and available, while maintaining integrity.
- HHS invests $7 billion annually in IT to support the wide-range of programs that the Department oversees and carries out as part of its mission.
- Information security professionals promote HHS' commitment to better health and well-being by ensuring information is kept secure.
- Understanding the security risks that information systems are exposed to and taking steps to mitigate them will result in a secure operating environment.



## Introduction

# Federal Information Security Management Act

- The Federal Information Security Management Act (FISMA) is the backbone of federal legislation regarding information security. It requires federal agencies to develop, document, and implement an enterprise information security program to cost-effectively reduce risks to IT assets.



Introduction

# Federal Legislation and Guidance

- Other important security and privacy legislation includes:
  - Clinger Cohen Act of 1996
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Privacy Act of 1974
  - Office of Management and Budget (OMB) Circular A-130
  - Paperwork Reduction Act
  - Children's Online Privacy Protection Act (COPPA)
- The National Institute of Standards and Technology (NIST) issues standards and guidelines to assist federal agencies in implementing security and privacy regulations.
- The Department uses NIST Special Publications (SP) and Federal Information Processing Standards (FIPS) to develop internal policies, procedures, and guidance. Special publications and FIPS can be found on the NIST Publication Portal.

## Introduction

# Department Governance

- The **HHS Cybersecurity Program** is the Department's information security program. Oversight is provided by the Office of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). The Program provides an enterprise-wide perspective, facilitates coordination among key stakeholders, sets standards and provides guidance to OpDivs, and supports streamlined reporting and metrics capabilities.
- **Operating Divisions** manage implementation of Department standards, provide business/domain expertise, develop policies and procedures specific to the OpDiv's operating environment, and manage ongoing operations.

# Information Security Overview

## Information Security Overview

# Introduction

- Individuals with responsibilities for the implementation and management of information systems must understand how their role relates to the information security program at the Department and OpDiv level.
- Such an understanding will enable mangers to perform their duties with a mindset of appropriate and adequate protection for HHS IT resources.

# Information Security Program Objectives

The overall objective of an information security program is to protect the information and systems that support the operations of the Department.

- To safeguard each system at HHS is to ensure that the following security objectives can be realized for their information:
  - **Confidentiality** - Protecting information from unauthorized access and disclosure.
  - **Integrity** - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.
  - **Availability** - Defending information systems and resources to ensure timely and reliable access to and use of information.

## Information Security Overview

# Threats

- Information systems are not perfect, nor are the people that interact with them, or the environments in which they function. As such, systems are vulnerable to misuse, interruptions and manipulation.
- A threat is the potential to cause unauthorized disclosure, unavailability, changes, or destruction of an asset.
- Threats can come from inside or outside HHS:
  - External forces can disrupt a system, such as a hacker maliciously accessing or corrupting data, or a storm disrupting power and network access.
  - An example of an internal threat is an employee who inappropriately changes, deletes, or uses data.

## Information Security Overview

# Vulnerability

- A vulnerability is any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.
- Some examples of vulnerabilities include:
  - Poorly communicated or implemented policy;
  - Inadequately trained personnel; and
  - Improperly configured systems or controls.

## Information Security Overview

# Risk

- A threat that exploits a vulnerability can allow information to be accessed, manipulated, deleted, or otherwise affected by those without the proper authority. It may also prevent data or a system from being accessed.
- Risk is the likelihood that a threat will exploit a vulnerability. For example, a system without a backup power source is vulnerable. A thunderstorm would create the threat of a power outage and increase the likelihood of system failure.
- Risk management is the process of identifying threats and vulnerabilities to IT assets and establishing acceptable controls to reduce the likelihood of a security breach or violation.

## Information Security Overview

# Security Controls

No information system is completely safe from threats, however controls help mitigate risks.

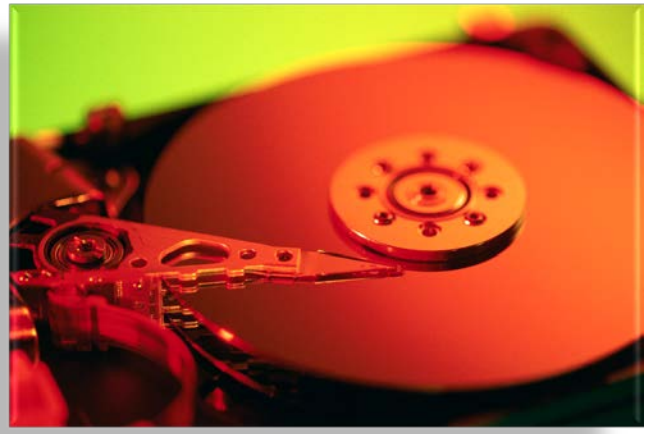
- Controls are policies, procedures, and practices designed to decrease the likelihood, manage the impact, or minimize the effect of a threat exploiting a vulnerability. Examples of controls include:
  - Clearly documented roles and responsibilities;
  - Security awareness and training program;
  - Incident response planning;
  - Physical security, like guards, badges, and fences;
  - Environmental controls in server rooms; and
  - Access controls, like PIV cards to log-on to the network.

## Information Security Overview

# Recap

- The goal of the information security program is to keep information and information systems confidential, available, and with integrity.
- The likelihood and impact of a threat exploiting a vulnerability is a risk to the system.
  - Example: Account privileges are not disabled when employees are terminated (vulnerability). A disgruntled former employee (threat) creates a risk that the organization's network and data will be compromised.
- There is an inherent risk in operating any information system. Controls help minimize and avoid some of the risk.

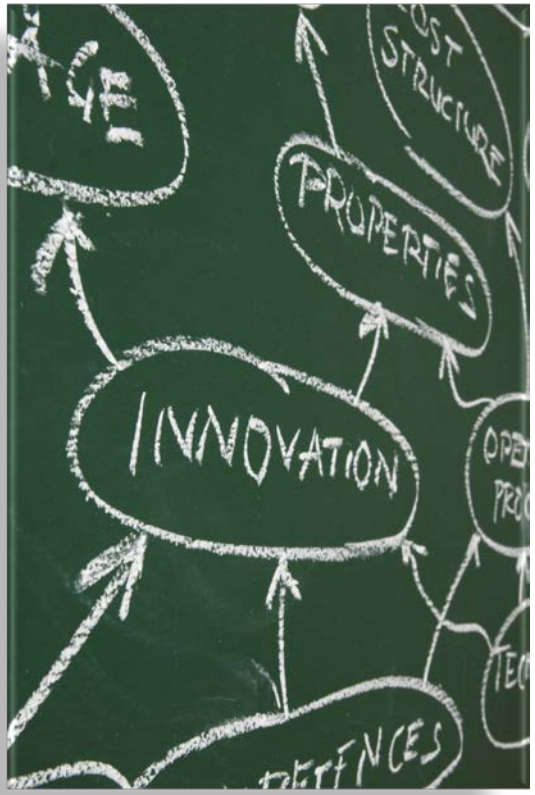
# Enterprise Performance Life Cycle



## Enterprise Performance Life Cycle

# Introduction

- The EPLC is a standardized project management methodology that guides HHS IT investments and ensures that mission objectives are being met throughout the lifetime of a system.
- Security is essential to developing or deploying a successful IT system. Information technology administrators, like yourself, should be part of the EPLC from the beginning.
- A detailed explanation of the EPLC can be found in the Enterprise Performance Life Cycle Framework Overview Document (http://www.hhs.gov/ocio/eplc/index.html).



## Enterprise Performance Life Cycle

# Phases

The EPLC consists of ten phases that guide the development process from initiation to termination.

**Ten Phases of the EPLC**

1. Initiation
2. Concept
3. Planning
4. Requirements Analysis
5. Design
6. Development
7. Test
8. Implementation
9. Operations & Maintenance
10. Disposition

## Enterprise Performance Life Cycle

# Benefits

- EPLC:
  - Ensures that IT projects have financial support throughout the life cycle;
  - Evaluates IT projects to determine whether they align with HHS and/or OpDiv goals;
  - Plans for and allocates part of the budget for system security from the beginning of the project; and
  - Determines that a similar IT asset does not exist, and the new project will meet the business need it is developed to address.
- The EPLC is flexible. Each phase can be tailored to meet specific characteristics of the project – taking in to account the size, duration, complexity of the project, etc.

## Enterprise Performance Life Cycle

# Stakeholders

- Stakeholders are an essential piece of the EPLC puzzle. There can be many stakeholders depending on the size and scope of the project. In general, every project will include:
  - Project Managers are responsible for planning, executing and overseeing phase activities. They also are responsible for creating the deliverables for review in conjunction with the Critical Partners.
  - Critical Partners are responsible for reviewing the project deliverables and validating policies in their functional areas.
  - IT Governance Organizations approve projects and monitor baselines and performance metrics throughout the life cycle. They also approve projects to advance to the next phase based on the recommendations of the Critical Partners.

## Enterprise Performance Life Cycle

# Deliverables

- The EPLC Framework Overview describes the documents and artifacts that need to be developed in each phase of the life cycle.
- Tailoring may reduce the level of effort and artifacts required for the phases. Changes to required documentation are identified in the Tailoring Agreement.
- For security documentation, at a minimum each system must have a System Security Plan (SSP), Risk Assessment, and Authorization to Operate (ATO).
- Documentation needs to be maintained throughout the life cycle of a system and should be stored accordingly.

## Enterprise Performance Life Cycle

# Stage Gate Reviews

- Approval of the project's key elements happen at Stage Gate Reviews during each of the ten phases.
  - Some reviews require governance oversight, while others are conducted internally.
- Stage Gate Reviews evaluate:
  - Successful accomplishment of phase objectives;
  - Plans for the next life cycle phase; and
  - Risks associated with transitioning to the next phase.
- Critical Partners are involved in the review and provide recommended actions to take place before the project moves to the next phase.

## Enterprise Performance Life Cycle

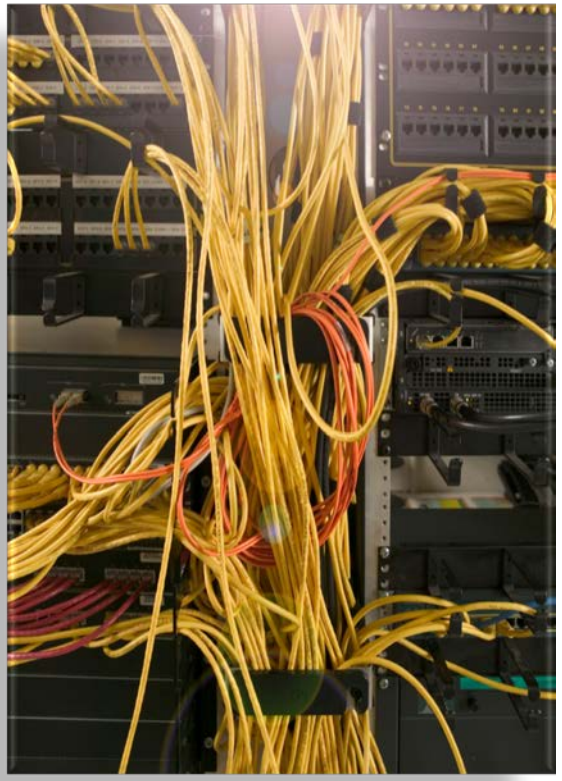
# Exit Criteria

- At the end of each phase, the project deliverables demonstrate evidence that the project has met the objectives of the phase.
- The EPLC Stage Gate Review Template lists the Mandatory Exit Criteria for each phase.

## Enterprise Performance Life Cycle

# Recap

- The EPLC is HHS' IT project management methodology.
- The EPLC ensures that IT systems meet business and mission objectives, are well managed, and cost-effective from inception to disposal.
- Building security into a system early in the design process is far more efficient than trying to add it on during or after development.
- Security Critical Partners ensure that security and privacy concerns are addressed during each phase of the life cycle.



# EPLC and the Risk Management Framework

## EPLC and the Risk Management Framework

# Introduction

- The RMF, as described in NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems, establishes a common risk management framework for all federal agencies to improve security and strengthen risk management processes.
- The RMF is a formal process used by HHS to ensure that security activities and artifacts are developed for all systems and applications at the right time.

## EPLC and the Risk Management Framework

# Risk Management Framework

At HHS, the RMF helps:

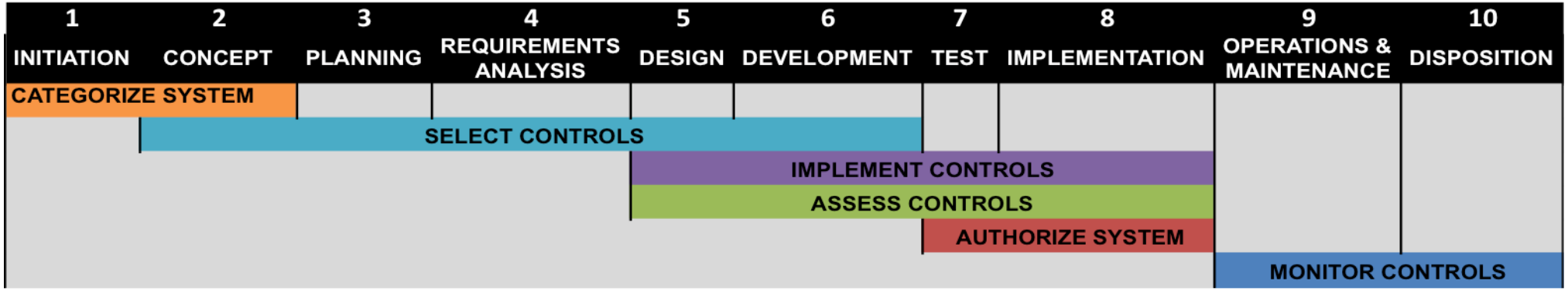
- Develop secure and compliant systems in a cost effective manner.
- Integrate security practices throughout the EPLC.
- Communicate security concepts and create a general understanding of security requirements.
- Provide support to project managers by helping them understand and comply with security requirements.

Source: NIST SP 800-37 Rev.1

## EPLC and the Risk Management Framework

# EPLC and RMF Integration

- The RMF is integrated into the EPLC so that IT security best practices and standards are built into a project from the beginning.
- The image below shows how the six steps of RMF are merged across the ten phases of the EPLC.



EPLC and the Risk Management Framework

# CATEGORIZE THE SYSTEM AND SELECT CONTROLS

During this step:
The system is categorized; and
Controls are selected based on the system categorization

## Categorize the System

# Risk Assessment

- **Risk assessment** or **risk analysis** is a process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
- The process incorporates threat and vulnerability analysis. It includes determining the likelihood that a security incident could occur, the resulting impact, and additional security controls that would mitigate this impact.
- Risk assessments should initially be conducted during the Initiation and Development stage of the EPLC. A risk assessment is also a required part of the security documentation for a security authorization.

## Categorize the System

# Determine Risk Impact Level

- FIPS 199 is used to determine the system categorization level of an IT system. Systems can be categorized as low, moderate, or high-impact for each of the security objectives: confidentiality, integrity, and availability.
- FIPS 200 is used to determine the system impact level, based on the categorization. Once the impact level is established, an appropriate set of controls, as identified in NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations can be chosen.
- NIST SP 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories is used to apply appropriate levels of controls for the system categorization.

## Categorize the System

# Risk Impact Assessment

FIPS 199 defines three categories of impact:

- **Low:** The potential impact is Low if the loss of confidentiality, integrity, and availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- **Moderate:** The potential impact is Moderate if the loss of confidentiality, integrity, and availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- **High:** The potential impact is High if the loss of confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

## Categorize the System

# High Water Mark

- The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well.
- According to FIPS 200, a “high water mark” is the highest potential impact value assigned to each security objective for each type of information resident on those information systems.

**Example 1**

A system has two moderate risk applications and one high risk application residing on it, the overall impact rating is high.

**Example 2**

A system is categorized as low for availability, low for integrity, but high for confidentiality, the overall impact rating is high.

## Select the Controls

# Control Selection

- Security controls are selected using NIST SP 800-53 Rev. 4 in combination with the low/moderate/high risk management guidance in FIPS 199 and FIPS 200.
- HHS security procedures and practices reflect the NIST and FIPS recommendations and requirements.

## Select the Controls

# System Controls

NIST SP 800-53 Rev. 4 divides controls into families. There are 18 security control families and eight privacy control families. In previous revisions, controls were organized in three classes - Management, Operational, and Technical. Although class designations have been eliminated from Rev. 4, it may be useful for an organization to apply them to individual security controls and their components.

- **Management Controls:** Focus on the management of the computer security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management, through policy and documentation.
- **Operational Controls:** Address security issues related to mechanisms primarily implemented and executed by people (as opposed to systems). Often, they require technical or specialized expertise and rely upon management activities as well as technical controls.
- **Technical Controls:** Technical controls are security controls that are configured within the system. Technical controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

## Select the Controls

# Security Control Families

| Management | Operational | Technical |
|---|---|---|
| • Security Assessments and Authorization<br>• Planning<br>• Risk Assessment<br>• System and Services Acquisition<br>• Program Management | • Awareness and Training<br>• Configuration Management<br>• Contingency Planning<br>• Incident Response<br>• Maintenance<br>• Media Protection<br>• Physical and Environmental Protection<br>• Personnel Security<br>• System and Information Integrity | • Access Control<br>• Audit and Accountability<br>• Identification and Authentication<br>• System and Communications Protection |

## Categorize the System and Select Controls

# Recap

- The categorization of the system directly effects the types of controls that are chosen for it.
- There are three categories of potential impact: low, moderate, or high.
  - These three categories determine how secure a system must be to ensure confidentiality, integrity, and availability.
- NIST SP 800-53 Rev. 4 contains a catalog of 18 security control families and eight privacy control families.

EPLC and the Risk Management Framework

# IMPLEMENT AND ASSESS THE CONTROLS

During this step:
Most of the security documentation is produced; and
Controls are tested.

## Implement the Controls

# System Security Plan

- The System Security Plan (SSP) for each system includes necessary information for the Authorizing Official (AO) to grant an ATO. The plan contains:
  - System identification, which includes the system owner, general description and purpose of the system, and equipment list;
  - A list of minimum security controls; and
  - Security documents that were developed during the EPLC.
- The SSP should be reviewed and updated or verified at least annually once the system is operational.
- If the system has changed (system environment, software, hardware, user groups, etc.), the SSP should be updated as soon as the change is made.

## Implement the Controls

# Contingency Plan

- A Contingency Plan for each system is required by law and includes the following key sections:
  - System criticality;
  - Responsibilities;
  - Business impact analysis;
  - Preventive controls;
  - Damage assessment;
  - Recovery and reconstitution; and
  - Backup requirements.

## Implement the Controls

# Configuration Management Plan

- Configuration management plans are documented for systems to ensure technical integrity of data within the system. Key components of the configuration management plan include:
- **Roles and Responsibilities** - Roles for system configuration management personnel and specific responsibilities (e.g., Executives, System Owners, Developers) are documented in detail.
- **Configuration Control Process** - Procedures are documented that specify the initiation, approval, change, and acceptance processes for all change requests.
- **Supplemental Configuration Management Information** - Information such as examples of change requests, explanation or user guidelines for automated configuration management tools should also be included in the plan.

## Implement the Controls

# Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an assessment process for identifying and mitigating the privacy risks posed by an information system. It is required for every system. At a minimum, PIAs must analyze and describe the following:

- What information is to be collected;
- Why the information is being collected (e.g., to determine eligibility);
- Intended use of the information (e.g., to verify existing data); and
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose).

## Implement the Controls

# Privacy Impact Assessment

Additionally, PIAs must include information on:

- When and how individuals can consent to or decline particular uses of the information (other than required or authorized uses);
- How the information will be secured (i.e., management, operational, and technological controls); and
- Whether a system of records is being created under the Privacy Act of 1974.

## Assess the Controls

# Security Control Assessment and Security Test & Evaluation

- A Security Control Assessment (SCA) is the formal evaluation of a system against a defined set of controls.
- It is conducted in conjunction with or independently of a full Security Test and Evaluation (ST&E), which is performed as part of the security authorization.
- The SCA and ST&E will evaluate the implementation (or planned implementation) of controls as defined in the SSP. The results are the risk assessment report. This report will document the system's areas of risk.
- Types of system tests conducted include audits, security reviews, vulnerability scanning, and penetration testing.

## Assess the Controls

# Plan of Action and Milestones

- Plan of Action and Milestones (POA&M) are a FISMA requirement to effectively manage security program risk and mitigate program-and system-level weaknesses.
- Effective POA&M management increases the awareness of an OpDiv's security posture, identifies systemic areas to address, and contributes to developing informed risk –based decisions.
- Every IT system should have a POA&M to identify, manage, and mitigate weaknesses.
- All security and privacy weaknesses shall be recorded and managed in the POA&M. Sources of these weaknesses can come from many locations such as audit reports, a security authorization cycle, and incidents.

## Assess the Controls

# Authorization to Operate

- Authorization is required before a system may process, store, or transmit Department data. An AO or a designated representative reviews the security authorization package. The AO or designated representative will then give a system either an ATO or Denial of Authorization to Operate.
- An ATO signifies completion of an objective third party system evaluation and acceptance of any residual risk of the system to the agency. This means that the AO takes responsibility if a security incident related to a known risk were to occur.
- Denial of Authorization to Operate indicates that there are major weaknesses or deficiencies in the security controls employed within or inherited by the information system. This rarely occurs if the processes outlined in the EPLC Framework Overview are followed.

## Implement and Assess the Controls

# Recap

- Most of the security documentation is finalized during this step.
- The documentation is used by the AO to determine if an ATO should be issued for the system.
- Every system must have an SSP, Risk Assessment, and ATO to operate. A POA&M is also required when weaknesses are identified.

EPLC and the Risk Management Framework

# MONITOR THE CONTROLS & SYSTEM DISPOSAL

During this step:
Controls are monitored and periodically tested; and
Plans are made to securely terminate the system.

## Monitor the Controls

# Configuration Management

- Once operational, systems are typically in a constant state of modification and enhancement, such as upgrades to components.
- Any change can have a significant impact on the security posture of the system. Therefore, continually documenting system changes and assessing the potential impact on the security is an essential aspect of maintaining system accreditation.
- Adherence to your OpDiv's configuration and change management procedures is necessary to maintain an accurate inventory of all changes to the system.

## Monitor the Controls

# Patch Management

- Part of maintaining a system is to ensure system components are kept up-to-date with patches. Effective patch management entails **maintaining an awareness of system vulnerabilities and available patches** for mitigation. Patches are periodically released for operating systems, office suites, commercial software tools and applications, and commonly used utilities.
- Patches should be **tested before deployment** to a production environment to prevent adverse impacts to operational systems.

## Monitor the Controls

# Continuous Monitoring

- FISMA requires periodic and continuous testing and evaluation of the security controls to ensure that they remain effective.
- The ongoing monitoring of security controls can be accomplished by one or a combination of the following:
  - Security review;
  - Security testing;
  - Evaluation or audit; and
  - Software/Hardware tools.

System Disposal

# Disposal of System Components

Media sanitization is important either at the end of the system's life cycle or at any point when new hardware or media is replacing existing hardware or media.

System disposal has five parts as stated in NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle*:

- **Building and Executing a Disposal/Transition Plan** ensures that all stakeholders are aware of the future plan for the system and its information. This plan should account for the disposal / transition status for all critical components, services, and information.
- **Information Preservation** ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.

## System Disposal

# Disposal of System Components (Continued)

- **Media Sanitization** ensures that data is deleted, erased, and written over as necessary to retain confidentiality.
- **Hardware and Software Disposal** ensures that hardware and software is disposed of as directed by the Information Systems Security Officer.
- **System Closure** ensures that the information system is formally shut down and disassembled.

For additional information, see the *HHS-OCIO Policy for Information Systems Security and Privacy* and *NIST SP 800-88, Guidelines for Media Sanitization*.

System Disposal

# Planning for Disposal

- Disposing of systems is a predictable occurrence. Planning ahead for the integration of security measures into the replacement process helps you securely and conscientiously manage both disposal and introduction of new hardware or software.
- Ensure that the purchase and installation of new equipment does not conflict with the proper disposal of data and old equipment. This prevents creating unnecessary vulnerabilities or an incident which could cause embarrassment to or damage the reputation of HHS.

- **Always take time to dispose of systems hardware and media properly!**

## Monitor the Controls & System Disposal

# Recap

- Once a system is operational, controls should be monitored for effectiveness and tested periodically.
- Changes in the configuration of the system could significantly impact security.
- It is critical to properly dispose of information systems and archive the data they contain. Plan and budget for disposal of the system early.

## EPLC and the Risk Management Framework

# Recap

- The six steps of the RMF are integrated across the ten phases of the EPLC to improve security and strengthen risk management processes.
- Each phase requires activities and deliverables to ensure that security is addressed throughout the life of the IT system.

# Summary

## Summary

# Conclusion

- Building security into a system early in the design process is far more efficient than trying to add it during or after development.
- Security is part of the foundation of a system. Resources are needed to design, develop, implement, and test the security features of the system.
- The EPLC and the RMF will ensure that security is an integral part of information systems at HHS.

## Summary

# Objectives

You should now be able to:

- ✓ Understand your role and responsibilities to protect information security as an HHS manager.
- ✓ Define the basic components of an information security program.
- ✓ Understand the EPLC and the RMF and how they relate to the development of IT systems.
- ✓ Identify where to locate HHS policies, procedures, and guidance for developing, implementing, and managing information systems from beginning to end.

## Appendix

# HHS Resources

- The **HHS Cybersecurity Program** is the Department's enterprise-wide information security and privacy program, helping to protect HHS against potential IT threats and vulnerabilities. The Program plays an important role in protecting HHS' ability to provide mission-critical operations, and is an enabler for e-government.
- HHS Cybersecurity Program Support provides assistance with IT security and privacy related questions. HHS Cybersecurity Program Support is staffed Monday through Friday from 8:00 AM to 5:00 PM eastern standard time (EST).

**Web**: HHS Cybersecurity Program

**Phone**: (202) 205-9581

**E-mail**: HHS.Cybersecurity@hhs.gov

## Appendix

# HHS Resources

- *HHS-OCIO Policy for Information Systems Security and Privacy*
- The *Enterprise Performance Life Cycle Frame*work *Overview Document* provides detailed information about how to complete each phase of the EPLC. It can be found at: http://www.hhs.gov/ocio/eplc/index.html.
- Templates, practice guides, checklists and other artifacts used throughout the EPLC process, including the Stage Gate Reviews template can be found at: http://www.hhs.gov/ocio/eplc/Enterprise%20Performance%20Lifecycle%20Stage%20Gate%20Reviews/eplc_stage_gate_reviews.html.

## Appendix

# Legislation and Guidance

- Legislation
  - E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
  - Federal Information Security Management Act (P.L. 107-347, Title III), December 2002
  - Paperwork Reduction Act (P.L. 104-13), May 1995.
- Standards
  - NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
  - NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006.

## Appendix

# Legislation and Guidance

- NIST Guidance
  - NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
  - NIST SP 800-27 Rev. A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.
  - NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
  - NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010.
  - NIST SP 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.
  - NIST SP 800-53 Rev. 4, Security and Privacy Controls for *Federal Information Systems and Organizations, April 2013.*

Appendix

# Legislation and Guidance

- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008.
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
- NIST SP 800-60, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
- NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle, October 2008.*
- NIST SP 800-70, Rev. 1, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2009.
- NIST SP 800-88, *Guidelines for Media Sanitization,* September 2006.

# Congratulations

You have completed the **Information Security for Managers** course.