Office of Chief Information Officer
Assistant Secretary for Administration
U.S. Department of Health and Human Services

Introductory Role-Based Training for IT Administrators - Training Transcripts

Foundational Training

Office of the Chief Information Officer
Assistant Secretary for Administration
U.S. Department of Health and Human Services

Acknowledgment

The majority of this training and its transcript document is based on the HHS Information Security Continuous Monitoring Strategy, V.2, dated May 2017. In some areas, the original text has been copied exactly and pasted into this document for consistency. We sincerely thank the authors of the above document, Mr. Christopher Bollerer and Mr. Bernard Asare from OCIO. Their document provided an expertise that greatly enriched the training.

We also thank NIST, OMB, SANS, GSA, the White House and additional resources listed in Appendix C for the content used within this training.

Many thanks to the HHS Privacy Team/HHS Policy Team/OHR Team for their assistance.

Table of Contents

Section 1 - Introduction

Welcome

The cybercrime landscape is evolving rapidly. The faster it expands, the more diligent IT professionals must become to stay on counteract new cyber threats. IT professionals are at the forefront of security as they respond to threats and fight continuously to ensure our virtual environments are secure. Due to the increased number of attempts to steal sensitive data, it is critical for the Department to integrate IT professionals' activities with risk management components to strengthen the overall information security program at HHS.

The overarching goal of this training is to ensure HHS IT Administrators possess the fundamental concepts to protect our information and information systems. This training contains the essential responsibilities required to perform the role of an IT Administrator.

Training Outline[1]

This training highlights three categories of responsibility for HHS IT Administrators. The first lesson is an overview of the HHS information security program; legislative and policy drivers that influence the program; and the risk management framework which governs the information security activities in HHS. The second lesson covers Continuous Monitoring Program strategies and lists the IT Administrators' responsibilities in each control monitoring stage of the program in more depth. The third lesson describes the IT Administrator's responsibilities and guidance on responding to incidents.

Training Objectives

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

- ❑ Identify the principles, governing bodies, risk framework and legislative drivers that shape the Information Security Program (ISP) in HHS.
- ❑ Maintain an ongoing awareness of system security status through the Information Security Continuous Monitoring (ISCM) Program.
- ❑ Respond to security incidents through applying established measures.

[1] *References to HHS information security policies, standards, and guidance are provided for the general use. Refer to your Operating Division's (OpDiv) security policies and procedures. In most cases they will be more specific than Department policy.*

Training Menu

Lesson 1: Information Security Program

- Information Security Program (ISP)
    - HHS Information Security Program (IS2P)
- Legislations, Policy Drivers and Standards
    - Federal Information Security Modernization Act of 2014 (FISMA)
    - FISMA Requirements
    - FISMA Metrics
    - Standards by NIST
- Risk Management
    - What is Risk?
    - Risk Factors
    - Risk Response
    - Risk Management Framework
    - Information Security Continuous Management Program (ISCM)

Lesson 2: HHS Information Security Continuous Monitoring Program (ISCM)

(Letters next to the header denote the Control Code in the ISCM Program)

- Information Security Continuous Monitoring Program (ISCM)
    - Security Controls
    - Your Responsibilities within the ISCM Program
- Your Responsibilities in ISCM Control Matrix
    - Account Management *(AC-2, 3, 6)*
    - Audit Review and Accountability (*(AU-6)*
    - Security Assessments *(CA-2)*
    - Continuous Monitoring *(CA-7)*
    - Baseline Configuration *(CM-2)*
    - Configuration Management *(CM-9)*
    - Contingency Planning *(CP-2)*
    - System Security Plan *(PL-2)*

Lesson 3: Incident Response

- Data Protection and Privacy
    - Controlled Unclassified Information (CUI)
    - IT Administrator's Role in Protecting CUI
- Security Incidents
    - What is an Incident?
    - Incident Handling Lifecycle
    - Incident Reporting Procedures
    - Roles in Incidents

Section 2 - Lessons

Lesson 1 – Information Security Program (ISP)

Overview

This lesson identifies the foundation of an Information Security Program. The legislative requirements will be explained including laws, policies, standards and documentation needed to securely operate and maintain the IT systems. The federal reporting requirements, and the framework used for federal information systems to define, monitor and address risks will also be discussed.

Objectives

- Describe security model and key concepts that built HHS Information Security Program.
- Recognize the legislations, regulations, standards and requirements governing HHS information security activities.
- Apply risk-based decisions based on the Risk Management Framework (RMF).

Topics

- Information Security Program (ISP)
    - HHS Information Security Program (IS2P)
- Legislations, Policy Drivers and Standards
    - Federal Information Security Modernization Act of 2014 (FISMA)
    - FISMA Requirements
    - FISMA Metrics
    - NIST Standards
- Risk Management
    - What is Risk?
    - Risk Factors
    - Risk Responses
    - Risk Management Framework (RMF)
    - Information Security Continuous Management Program (ISCM)

Information Security Program (ISP)

An **Information Security Program (ISP)** is required by law. The overall objective of an information security program is to protect the information and information systems that support the operations and assets of the organization. As an IT Administrator, you are a core component of the HHS ISP and you play a vital role in safeguarding the HHS information assets.

HHS Information Security Program (IS2P) [2]

To meet the federal requirements, the Department instituted policies and procedures, known as the HHS Policy for Information Systems Security and Privacy (IS2P), to safeguard information stored, processed and/or transmitted. HHS Chief Information Officer (CIO) and Chief Information Security Officer (CISO) oversee the Department's information security program entitled "HHS Cybersecurity Program." The goal of the program is to establish a risk-based information security program that is compliant with the Federal Information Security Modernization Act of 2014 (FISMA); the recommendations and standards detailed by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB) memoranda; as well as the Presidential Directives (PD).

Operating Divisions (OpDivs) manage the implementation of the Department's standards, provide business/domain expertise, develop policies and procedures specific to their operating environment, and manage ongoing operations.

Pop-up Window: Components of the security program in HHS.

- Security Governance
- System Development Life Cycle (SDLC)
- Awareness and Training
- Capital Planning and Investment Control
- System Connections
- Performance Measures
- Security Planning
- IT Contingency Planning
- Risk Management
- Security Assessment and Authorization
- Incident Response
- Security Services and Product Acquisitions
- Configuration Management
- Continuous Monitoring
- Vulnerability and Patch Management

Legislations, Policy Drivers and Standards

Federal Information Security Modernization Act of 2014 (FISMA)[3]

FISMA is the backbone of federal legislation regarding information security. It establishes requirements for the implementation of security controls and requires annual assessments of the efficacy of those controls. It also assigns specific responsibilities to federal agencies, National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB), to strengthen information security systems.

---

[2] *HHS Information Security and Privacy Policy (IS2P) link: http://intranet.hhs.gov/it/cybersecurity/policies/index.html. Users need to create an account in MAX to be able to read through the policy.*

[3] *Federal Information Security Modernization Act of 2014 (FISMA): https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.*

According to FISMA, the term *information security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Under FISMA, NIST has statutory responsibilities to develop standards, guidelines, and associated methods and techniques for providing adequate information security for all agency assets and operations, excluding national security systems.

FISMA Requirements

FISMA requires the head of the agency to implement policies and procedures to cost-effectively reduce IT security risks to an acceptable level. If the agency continually under-performs or does not report metrics, OMB may withhold funding. FISMA requirements are:

- System Security Plan (SSP): Each system requires an SSP to document security planning, system and component attributes, and implementation of baseline security controls for the information system.
- Plan of Action and Milestones (POA&M): Each system must have a POA&M for documenting, tracking, and mitigating security deficiencies/weaknesses. System owners or representatives must report on the progress against security deficiencies identified in the POA&M.
- Assessment and Authorization: During the "authorize" phase of the RMF, the Authoring Officer (AO) determines that the system has an acceptable risk level and grants an Authority to Operation (ATO). Traditionally, system ATOs have an expiration date of a maximum three years.
- Continuous Monitoring: FISMA requires that the controls implemented are constantly improving or remain in place, and that documented weaknesses are timely and effectively mitigated.
- Audit: systems should be assessed by Inspector General (IG) office annually.

FISMA Metrics

FISMA metrics are based on the Cybersecurity Framework established by NIST[4]. The metrics leverage the Cybersecurity Framework as a standard for managing and reducing cybersecurity risks, and they are organized around the framework's five functions: Identify, Protect, Detect, Respond and Recover.

HHS continuously evaluates these metrics; and OpDivs report their metrics to OMB, quarterly. OMB measures the quality of agency programs, policies, and procedures to see if they comply with the president's policies. The Office of the Inspector General (OIG) audits information security policies and procedures annually.

Pop-up Window: FISMA metrics.

IDENTIFY your inventory of government furnished equipment (GFE) and other hardware and software systems and assets, which are connected to the networks. Identifying these systems and assets helps agencies facilitate their management of cybersecurity risks to systems, assets, data, and capabilities.

[4] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

PROTECT and ensure that HHS safeguards its systems, networks, and facilities with appropriate cybersecurity defenses. The protect function supports the agencies' ability to limit or contain the impact of potential cybersecurity events.

DETECT metrics assesses the extent that the agencies are able to discover cybersecurity events in a timely manner. Agencies should maintain and test intrusion-detection processes and procedures to ensure they have timely and adequate awareness of anomalous events on their systems and networks.

RESPOND metrics ensures that agencies have policies and procedures in place that detail how their enterprise will respond to cybersecurity events. Agencies should develop and test response plans and communicate response activities to stakeholders to minimize the impact of incidents when they occur.

RECOVER metrics ensures that agencies develop and implement appropriate activities for resilience that allow for the restoration of any capabilities and/or services that were impaired due to an incident. The recover function reduces the impact of the incident through the timely resumption of normal operations[5].

Brain Teaser - 1
The metric that evaluates the agency's capability to discover cybersecurity events in a timely manner is called: _____

A. Identification
B. Response
C. Detection
D. Assessment

Answer: C
Explanation: Agencies should maintain and test intrusion-detection processes and procedures to ensure they have timely and adequate awareness of anomalous events on their systems and networks.

Standards by the National Institute of Standards and Technology (NIST)
NIST is responsible for developing standards and guidelines, including baseline security requirements, for the protection of all agencies' operations and assets. NIST works closely with federal agencies to improve their understanding and implementation of FISMA requirements and publishes standards and guidelines which provide the foundation for strong information security programs for all agencies. NIST uses three Special Publication (SP) series to publish computer/cyber/information security guidelines, recommendations and reference materials: SP 800, 1800, 500. HHS focuses on NIST SP 800 series[6].

Along with these legislations, there are other federal resources that help build an effective security program, and influence the Department's technological infrastructure and information asset safeguards.

[5] https://www.dhs.gov/sites/default/files/publications/FY%202017%20CIO%20FISMA%20Metrics-%20508%20Compliant.pdf
[6] *A list of the NIST publications can be found http://csrc.nist.gov/publications/PubsSPs.html*

Pop-up Window: List of federal and national references.

IT Legislation and Guidance

- Federal Information Security Modernization Act (FISMA) of December 2014
- E-Government Act of 2002
- Clinger-Cohen Act
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- Office of Management and Budget (OMB) Circular A-130

Privacy Legislation

- Privacy Act of 1974
- Paperwork Reduction Act of 1974
- Children's Online Privacy Protection Act (COPPA)
- Electronic Communications Privacy Act (2015-2016

Presidential Directives

- Presidential Executive Order on Strengthening Cybersecurity of Federal Networks and Critical Infrastructure

Risk Management

What is Risk?

Risk is the likelihood that a threat will exploit vulnerability. For example, a system without a backup power source is considered vulnerable and has a risk of exploitation. A threat, such as a thunderstorm, would increase the likelihood or risk of a power outage and creates a risk of system failure.

Risk Factors

A threat is the potential to cause an unauthorized access, access denial, disclosure, changes, or destruction of an information asset. Threats come from inside or outside HHS. External forces can disrupt a system, such as a storm disrupting power and network access, while the internal threat can be an employee who inappropriately changes, deletes, or uses data. A threat that exploits a vulnerability, allows information to be accessed, manipulated, deleted, or otherwise affected by those without the proper authority. 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.

Brain Teaser - 2

A co-worker who is recently hired as an IT specialist told you that she granted system access to an employee without checking the user's authorized access level. Is that access considered to be a risk?

A. Yes B. No

Answer: Yes.

Explanation: Granting access to HHS information systems without confirming the user's authorized access level is considered an improper configuration of the security control. It is a vulnerability and may pose a threat.

Risk Response

Responding to risks varies in each level. At the system level, risk response may include implementation of additional controls, modifications to implemented controls, removal of a system's Authority-to-Operate (ATO), changes to the control monitoring frequencies, and/or additional analysis of security-related information. At the OpDiv/StaffDiv level, risk response may include requests for additional security-related information, new or modified metrics, changes in mission/business processes; changes to information system reporting requirements, and/or additions or modifications to common control implementations. Finally, at the Department level, risk response may include changes to security policies.

Risk Management Framework (RMF)

Risk management[7] 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. The RMF, as described by NIST[8], establishes a common risk management framework for all federal agencies to improve security and strengthen risk management processes. It applies to the organization's mission and information systems perspectives; and provides a disciplined and structured process that integrates information security and risk management activities.

The RMF at HHS helps communicate security concepts and creates a general understanding of security requirements. It also ensures that security controls are integrated into information systems while they are being designed, being operated, and when removed from operations.

Pop-up Window: Risk Management Framework chart.

Step 1: Categorize information system: Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

Step 2: Select Security Controls: Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

Step 3: Implement Security Controls: Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

Step 4: Assess Security Controls: Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements for information system).

Step 5: Authorize Information Systems: Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

Step 6: Monitor Security State: Continuously track changes to the information system that may affect security controls and reassess control effectiveness[9].

---

[7] *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

[8] *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.*

[9] *http://csrc.nist.gov/groups/SMA/fisma/documents/risk-management-framework-2009.pdf*

Knowledge Check

Which of the following tasks in the RMF process determines the security impact of any changes to the information system and its operation?

A. Continuous monitoring
B. Ongoing security controls assessment
C. Select security controls
D. Establishing security levels

Answer: A.

Explanation: Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is a crucial element of an effective security control monitoring.

Information Security Continuous Management Program (ISCM)

The OMB requires federal agencies to manage information security risk on an ongoing basis[10]. NIST defines ISCM as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." ISCM is integrated in the RMF phases and occurs at step 6: "Monitor" phase. The program supports the monitoring of security controls in near-real time and helps organizations assess and authorize information systems. Each OpDiv defines metrics that align with their information security goals and identify improvements to the security posture of the system.

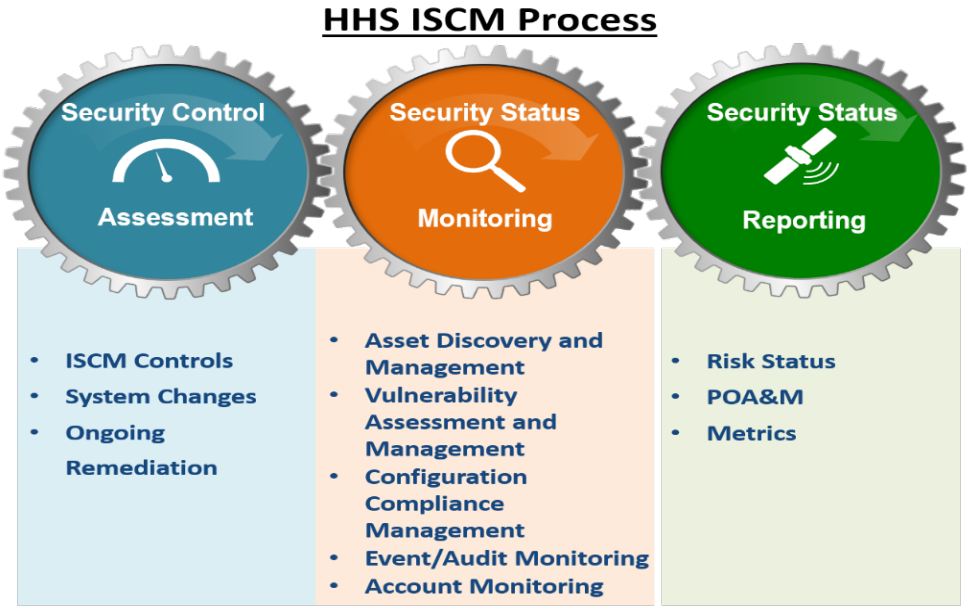

Figure 1: Link to image description

Lesson Summary

There are laws, regulations, and statutory bodies that establish requirements and develop mechanisms to safeguard the federal information systems and assets. The development and execution of organizational security policies and standards maximize compliance and minimize risks. Noncompliance, however, may result in withholding funds as well as exposing the organization to public distrust.

[10] *https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf*

There is an inherent risk in operating any information system. There are also numerous controls used to deter and mitigate risks. A well-designed risk management framework helps identify and reduce the risks before they even happen. IT Administrators play a supporting role in the overall risk management process by continuously monitoring and updating security controls.

Lesson Quiz

1. Which of the following is the IT administrator's role in the RMF process:
   A. To ensure appropriate security requirements are implemented and enforced for all systems or networks.
   B. To identify security impacts associated with system implementation procedures.
   C. To provide support, particularly in the implementation and monitoring steps in the RMF process as it applies to your information system.
   D. All of the above.

Answer: D.

2. The _____ is the document that comprises all the security systems components; attributes; risk factors and implementation of baseline security controls for the information system.
   A. POA&M
   B. Risk Management Framework
   C. System Security Plan (SSP)
   D. CIA Triad

Answer: C

3. A former Help Desk employee obtained a job on the Incident response team in the same HHS OpDiv. While in his new job role he noticed he still has administrative access to remotely log in to workstations within his OpDiv. Does that constitute a potential threat?
   A. No, it's not a threat. He's still our employee.
   B. Yes, it's a threat, although he's our employee.
   C. Don't know.
   D. Something else.

Answer: B

Lesson 2 – HHS Information Security Continuous Monitoring Program (ISCM)

Overview

To maintain an ongoing monitoring of the information system, HHS has developed the ISCM program that helps prioritize risk consistently and addresses how the agency conducts ongoing authorization of information systems and its environment. This lesson is divided into two parts. The first part elaborates on the ISCM program and the IT Administrator's overall role within the program. The second part details monitoring controls set by ISCM and the IT Administrator's tasks to fulfill them.

Objectives

- Recognize ISCM Program's baseline requirements.
- Identify the IT Administrator's responsibilities in ongoing monitoring.
- Apply effective tools for security monitoring and reporting.

Topics

(Letters next to the paragraph header denote the Control Code in the ISCM Program)

- Information Security Continuous Monitoring Program (ISCM)
    - Security Controls
    - Your Responsibilities within the ISCM Program
- Your Responsibilities in ISCM Control Matrix
    - Account Management *(AC-2, 3, 6)*
    - Audit Review and Accountability (*(AU-6)*
    - Security Assessments *(CA-2)*
    - Continuous Monitoring *(CA-7)*
    - Baseline Configuration *(CM-2)*
    - Configuration Management *(CM-9)*
    - Contingency Planning *(CP-2)*
    - System Security Plan *(PL-2)*

Information Security Continuous Monitoring (ISCM)

The ISCM entrusts IT personnel with the responsibility of ongoing monitoring of security controls and recording any relevant information about specific changes to hardware, software, and firmware. IT personnel are also responsible for modifications to hosting networks and facilities, threats, misuse of the system; and changes to the organization's risk plans. This information is used to assess the potential security impact of those changes[11] on the security controls for early risk detection.

Pop-up Window: HHS ISCM Implementation Process chart.

[11] *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

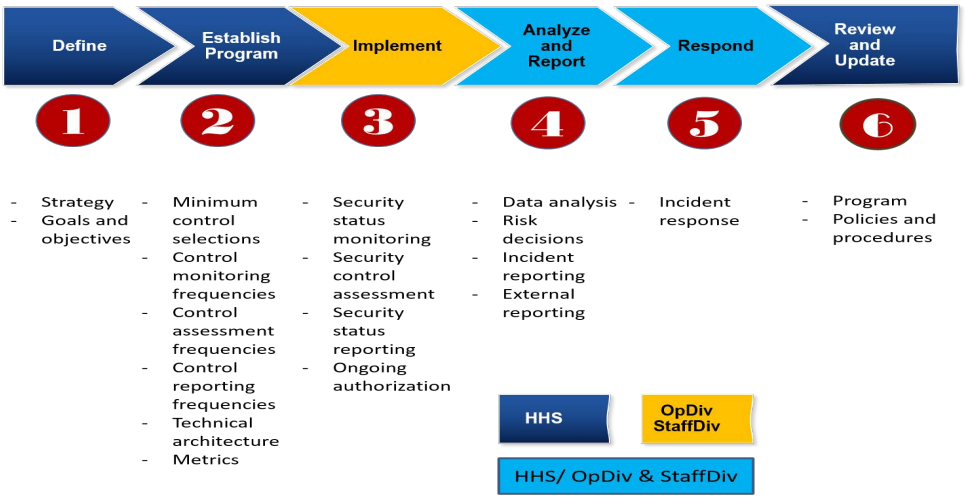

Figure 2: Link to image description

Security Controls

Security controls as defined by NIST are "technical or administrative safeguards or counter measures to avoid, counteract or minimize loss or unavailability due to threats." Federal organizations must meet the security baseline requirements by selecting the appropriate security controls set by FIPS 200[12]. There are three different types of security controls[13].

Pop-up Window: Types of security controls:

- **Common Controls**: Shared by more than one system or inherited from another system. Contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls are excellent examples for common controls.
- **Hybrid Controls:** Any combination of "common" controls; and "system-specific." Controls to form one control. For example, the organization may choose to implement the Contingency Planning security control by providing a template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific uses.
- **System-specific Controls:** Specific to one system and the System Owner has the responsibility to implement. An example of a system-specific control is the authenticator feedback, where the information system is designed to obscure the feedback of authentication information during the authentication process. For example, the displaying of asterisks when a user types in a password. Asterisks are used to obscure the feedback of authentication information.

Your Responsibilities within the ISCM program

IT Administrators create partnerships and collaborate with senior leaders and network administrators to confirm the system security meets Department standards. Significant changes to the organizational risk management strategy, information security policy, supported missions functions require an immediate assessment of the security status of the information system and, if necessary, a modification or update to the current security controls.

[12] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
[13] http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/select/faq-Select-step2.pdf (P.8)

Your role is to ensure that security controls are implemented; and the appropriate security requirements are enforced. You also need to identify the security impacts associated with those changes; and assess the performance of the security controls to ensure that the residual risk is within an acceptable range[14]. The specifics of your role can be:

- Participate in the HHS configuration management process;
- Establish and maintain an inventory of components associated with common controls;
- Conducts security impact analyses on changes of the common controls;
- Prepare and submit security status reports in accordance with HHS policy and procedures;
- Conducts remediation activities as necessary to maintain common control authorization;
- Updates/ revises the common security control monitoring process as required;
- Updates critical security documents as changes occur; and
- Distributes critical security documents to individual information owners/ information system owners, and other senior leaders in accordance with HHS policy and procedures.

Your Responsibilities within the ISCM Control Matrix

In addition to monitoring the control frequencies, the ISCM program identifies some monitoring methods, such as: continuous monitoring plans; account management; configuration settings; audit and accountability; contingency planning; security assessment; and system security plans. In each of these methods, the IT Administrator is a major contributor to the successful fulfillment of the control.

Account Management *(AC-2, 3, 6)*

As part of management controls, all information systems must perform an annual review and recertification of user accounts to verify if the account holder requires continued access to the system. User's access controls limit the rights of authorized users, systems, applications, or processes and prevent unauthorized use of a resource or use of a resource in an unauthorized manner.

As an IT Administrator, you should have two accounts: A normal user account and an Administrator account. Your Administrator privileged account should only be used when you need an Administrator privilege to perform a job function- otherwise this account level should not be in use.

For account management of all users you need to:

- Ensure segregation of user and administrator accounts.
- Implement, monitor, remove and re-certify user access on a continual basis;
- Review the user's access on a defined recurrence and report it to the ISSO and/or supervisor;
- Periodically recertify the users' access to ensure the system access is limited to those who have a current business purpose; and that there is no excessive or unusual number of individuals receiving administrator-level access. These access irregularities could indicate a lack of controls; and

[14] *See the HHS IS2P document to see a list of controls and IT Administrator responsibilities.*

- Disable the accounts that are terminated within an OpDiv-defined timeframe unless written certification of the need for continuation of access is obtained. Accounts for separated employees, contractors, volunteers or others who are no longer requiring access are terminated immediately. For potentially hostile terminations, access is terminated at the exact time of employee's notification.

Audit Review and Accountability *(AU-6)*

FIPS 200 stipulates that organizations must create, protect, and retain information system audit records and ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. The IT Administrators are involved in the preparatory phase that precedes systems' audits; and their task is to ensure an adequate secure inspection process through:

- Reviewing audit records frequently for signs of unauthorized activity; and other security events;
- Ensuring all documentation, including the SSPs, are up to date and remediate any open POA&M item;
- Retaining an up to date list of security activity logs and system maintenance reports and results;
- Creating a report of all users with system access and with elevated privileges;
- Reviewing hardware and software inventory to ensure it is up to date; and
- Identifying and discussing with stakeholders any incidents or unplanned system events.

Brain Teaser - 1

An IT administrator is responsible for enabling file access on the network for a group of users. From your experience and what you've learned thus far, which of the following actions is unnecessary for this task?

A. Identify user's access level.
B. Installing and monitoring patches.
C. Assess the privilege level access and confirm user's eligibility.
D. Identification and authentication of users.

Answer: B.

Explanation: Before enabling access to a network file, the IT Administrator should identify user's access level; assess privilege level access and confirms user's eligibility to receive the network file.

Security Assessments *(CA-2)*

Security control assessments are conducted during the initial installation and annually thereafter. Common events may trigger IT Administrators to modify controls. Administrator's intervention may happen when:

- A new or modified hardware or software (including applications and operating systems) is hosted;
- New threats introduced to the environment; and
- Optimization or system changes.

Continuous Monitoring Plan *(CA-7)*

A Continuous Monitoring Plan must be developed for each system and updated annually to maintain ongoing authorization of the system. The goal of continuous monitoring is to obtain a highly secure posture and then maintain the status once you've reached it. Continuous monitoring involves:

- Identifying the information security system's issues or hardening the system to meet security requirements for the operational environment in which they reside;
- Installing and monitoring patches and updates to systems and continuously checking the system to ensure that the up-to-date patches are applied; and the performance parameters are always optimal;
- Managing user level access and running scans and reviewing logs. Logs can be used to detect suspicious activities, operationally and technically; and
- Being vigilant and cognizant of normal usage patterns and discerns changes. Some examples of abnormal usage patterns can be: activity late at night outside of the normal traffic pattern; an individual asking others for their password or other credentials; large amounts of data leaving the network; or, user accounts getting locked excessively or by individuals temporarily absent.

Brain Teaser - 2

Your ISSO decided to upgrade the security control baseline. As an IT Administrator, do you need to upgrade the technical controls following this upgrade?

A. Yes B. No

Answer: A.

Explanation: IT Administrators are in charge of implementing the technical controls following changes to the RMF or any changes to the organization's mission.

Baseline Configuration *(CM-2)*

This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters); network topology, and the logical placement of those components within the system architecture.

Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. As an IT admin, there are many roles associated with implementing an effective CM process, some of which are:

- Document and implement the CM plan;
- Establish system baselines and evaluate controls;
- Ensure that proposed changes do not adversely affect agency systems or data;
- Manage change requests and coordinatie implementation of changes;
- Notify users of system changes and conduct impact analysis of changes;
- Ensure existence of a process for storing, retrieving, and distributing CM materials; and an audit trail of changes is documented and maintained.

Configuration Management *(CM-9)*

The Configuration Management plan establishes a means for identifying configuration items (hardware, software, firmware, documentation) throughout the system development life cycle and a documented process for managing system changes through the change management process. The IT Administrators are critically important for a successful change, installation or transition of an information system. They ensure the security measures remain in place during installation and/or transition through:

- Account validation through disabling unused or unknown accounts;
- Remote access verification and confirmation that the remote access is authorized before allowing it;
- Physical access to keep devices secure and monitoring physical access where applicable;
- Files configuration and checking the settings before putting the system in operation; and
- Hardening the systems during the setup and during re-establishment[16].

Contingency Planning *(CP-2)*

The Contingency Plan needs to be updated and tested at least annually or when significant changes occur to the system. Your duties for contingency planning are as simple as:

- Developing and maintaining a contingency plan specific to your information system;
- Ensuring data backup practices are being completed and the backed up data is re-usable; and
- Maintaining a supply of hardware/ software and keep spare equipment refreshed.

Knowledge Check

You have been tasked by your supervisor to monitor the accounts of a group of users in one of the HHS medical research laboratories when you notice that a large amount of data leaves the network at night. Which task below is required when monitoring this particular situation?

A. Patching the operating system
B. Updating Office suites on the laboratories' computers
C. Review the hardware and software inventory.
D. None of the above

Answer: D.

Explanation: A large amount of data leaving the network at night is an abnormal activity that warrants your vigilance and immediate action. In that case, follow the established procedures set by the Department's or your OpDiv's system security plan if there's a need to change the security controls.

System Security Plan (SSP) *(PL-2)*

Poorly implemented controls or controls that did not have a control measure implemented are considered weaknesses and must be documented in the Plan of Action and Milestones (POA&M). IT Administrators are often responsible for controls that are implemented or addressed in the SSP. If a control cannot be implemented, the reason must be documented in the plan; and it should have one of the following annotations: Not Applicable; POA&M; or Accepted Risk. Any accepted risk, exception, or deviation must be

[16] *Each OpDiv has their specific baseline or hardening parameters to implement during installation.*

approved. IT Administrators work with ISSO to create and monitor the POA&M and ensure that the controls that are not fully implemented are still addressed in a cost-effective and risk-based fashion.

Pop-up Window: POA&M definition.

Plan of Action and Milestone (POA&M)

The POA&M document is a FISMA requirement to effectively identify and manage security program risk and system-level weaknesses. 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 may come from some venues as: audit reports, a security authorization cycle, and incidents.

Lesson Summary

As a steward of the HHS Information and information systems, you are responsible for maintaining the baseline requirements for securing the HHS information assets and systems. As such, you are entrusted with the technical implementation of security controls and addressing technical changes in the security plans. Your contributions to the ISCM Program, in various security control monitoring activities, are indispensable. After all, HHS depends on IT Administrators to maintain a secure network environment at all times.

Lesson Quiz

1. Awareness of system vulnerabilities is an important component in the:
    A. Contingency Management
    B. Change Management
    C. Media Sanitation
    D. Patch and Update Management

Answer: D

2. The POA&M lists all:
    A. Log in and out activities
    B. System security plans
    C. Security and privacy weakness
    D. None of these

Answer: C

3. In one of your periodic checks on a user's access, you noticed the number of the individuals who have administrator-level access increased significantly in comparison to last period's numbers. What does that mean?
    A. An indicator of stable and secure system.
    B. Fewer users can make changes to the information system.
    C. A lack of enough security controls.
    D. An increase in the number of users who had been promoted to executive positions.

Answer: C

Lesson 3 – Incident Response

Overview

Data is knowledge and knowledge is power. According to the Department of Justice's website, the health care data fraud estimate was close to $100 billion a year. As powerful as it is, data exploitation intrigues more hackers, and the data schemes continue to grow in complexity and seriousness. That's why data protection is extremely vital at HHS. This lesson discusses the different types of data stored in our information systems; the value of this information; how to detect possible incidents; incidents' lifecycle; and your role as an IT Administrator when that data is compromised.

Objectives

- Define the Controlled Unclassified Information (CUI) types.
- Initiate incident handling actions based on your responsibilities as an IT Administrator.
- Respond to incidents according to established techniques and methodologies.

Topics

- Data Protection and Privacy
  - Controlled Unclassified Information (CUI)
  - IT Administrator Role in Protecting CUI
- Security Incidents
  - What is an Incident?
  - Incident Handling Lifecycle
  - Incident Reporting Procedures
  - Roles in Incidents
  - IT Administrator's Role in Incident Handling
  - Privacy Incident Response Team

Data Protection and Privacy

The Federal laws protect the privacy of individuals and mandate organizations to secure the sensitive data they routinely process, store or transit about the individuals. The confidentiality impact level that every organization securely maintains the sensitive data determines how far this organization is successful in carrying its mission while retaining the public trust.

Controlled Unclassified Information (CUI)

CUI[17] is information that has a degree of confidentiality such that its loss, misuse, unauthorized access, or modification could compromise the element of confidentiality and thereby adversely affect national health interests and the operation of HHS programs. CUI includes, but is not limited to, Personally Identifiable Information (PII) and Protected Health Information (PHI). In this training, we will refer to sensitive data as CUI.[18] PII and PHI should be protected from inappropriate access, use, and disclosure. This also includes data located in multiple locations (e.g. databases, shared network drives, backup tapes, contractor sites) and in any format (written or audio) and via any transmission means.

[17] *https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information*

[18] *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf*

Pop-up Window: Definitions of PII and PHI.

Personally Identifiable Information (PII)

The PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples include: name, phone number, address, Social Security number, date and place of birth, mother's maiden name, biometric records, and medical information.

PII in your information system should be assigned a confidentiality impact level and associated policies, procedures and training should be developed to govern its use.[19]

Protected Health (PHI)

PHI is any individually identifiable health information that is collected, used or circulated by an entity that falls under the governance of HIPAA as clinic offices; medical facilities; laboratories; health insurance providers; etc.[20]

IT Administrator's Role in Protecting CUI

To safeguard CUI, you first need to recognize PII and PHI data in your information system and then secure it by:

- Minimizing access to data based on the need-to-know, approve access only as required by policy;
- Monitoring the use of information systems and devices where CUI is stored, used or transmitted;
- Supporting media transport and sanitization when PII and PHI are no longer required for the mission;
- Ensuring encryption is configured correctly and the audit parameters are turned on and properly reported according to the policy; and
- Implementing and monitoring the security controls; and, when necessary, apply additional controls above the baseline controls to help safeguard CUI confidentiality.

Brain Teaser - 1

While reviewing the access logs of the patient medical records management system, you noticed that a medical transporter logged into the system late at night. Medical transporters in this facility are required to move patients between treatment rooms and the hospital floor only. However, the logging activity lingered to 30 minutes and the transporter accessed information about patient's names, health insurance ID, lab results and medical history. Is this a violation of HIPAA?

A. Yes B. No

Answer: Yes, it is.

Explanation: By reviewing the patient's history and lab results, the employee viewed more information than what he needed to know to perform his duty as a medical transporter between the hospital floors. He actually gained an unauthorized access to the patient's PHI and in doing so; he violated HIPAA regulations and security policies.

[19] *References: OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information and NIST SP 800-122 Guide to Protecting the Confidentiality of PII.*

[20] *What health information protected by privacy rules? https://privacyruleandresearch.nih.gov/pr_07.asp*

Explanation: By reviewing the patient's history and lab results, the employee viewed more information than what he needed to know to perform his duty as a medical transporter between the hospital floors. He actually gained an unauthorized access to the patient's PHI and in doing so; he violated HIPAA regulations and security policies.

Security Incidents

What is an Incident?

An incident is an occurrence that actually or imminently jeopardizes the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[21]

Incident examples include: attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; or changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Breaches involving CUI receive considerable media attention and negatively affect an organization's reputation. These types of breaches can also shake the public's faith in the organization's ability to protect CUI.

FISMA requires Federal agencies to have procedures for handling information security incidents; and directs OMB to establish a central Federal information security incident center: U.S. Computer Emergency Readiness Team (US-CERT).

Incident Handling Lifecycle

NIST sets the following procedures for handling incidents[22]:

- Preparation: It ensures the proper policies and procedures, lines of communication and team members are identified prior to an incident occurring.
- Detection & Analysis: Known as "Identification" at HHS. It is identifying and differentiating an incident from an event. This includes gathering, and triaging of all available data associated with the incident.
- Containment, Eradication, and Recovery: It initiates the seclusion of affected hosts and systems from the network, initiates network blocks on adversaries, addresses issues; and then brings the network/system back to production status.
- Post-Incident Activity: Known as "Lessons Learned" at HHS. In this step, notes and lessons learned from the response are evaluated; and in turn, used to improve the security landscape by enhancing patching methodologies, re-evaluating access permissions, account usage, and user's training.

[21] *OMB Memorandum M-17-12*

[22] *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

Brain Teaser - 2

Triaging all the information that accompanied an event in order to differentiate an incident from an event is called which of the following terms at HHS? _____

A. Preparation
B. Containment
C. Identification
D. Assessment

Answer: C.

Explanation: This procedure is called Detection & Analysis and known as "Identification" at HHS. It is identifying and differentiating an incident from an event. This includes gathering, and triaging of all available data associated with the incident prior to the final determination.

Incident Reporting Procedures[23]

Immediate and effective reporting helps prepare for future incidents, and prevents them from reoccurring. Incident reporting shares knowledge across OpDivs and reduces the likelihood of future occurrences. Be sure to follow incident reporting procedures while an incident is being handled and document each step toward resolution.

Pop-up Window: Incident Handling Checklist that HHS uses for handling its incidents. The list provides guidelines to handlers on the major steps that should be performed in case of a cybersecurity incident. It does not dictate the exact sequence of steps that should always be followed. The actual steps performed may vary based on the type of incident and the nature of individual incidents.

Detection and Analysis	
1.	Determine whether an incident has occurred.
1.1	Analyze the precursors and indicators.
1.2	Look for correlating information.
1.3	Perform research (e.g., search engines, knowledge base).
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.).
3.	Report the incident to the appropriate internal personnel and external organizations.
Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence.
5.	Contain the incident.
6.	Eradicate the incident.
6.1	Identify and mitigate all vulnerabilities that were exploited.

[23] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

6.2	Remove malware, inappropriate materials, and other components.
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them.
7.	Recover from the incident.
7.1	Return affected systems to an operationally ready state.
7.2	Confirm that the affected systems are functioning normally.
7.3	If necessary, implement additional monitoring to look for future related activity.
Post-Incident Activity	
8.	Create a follow-up report.
9.	Hold a "lessons learned" meeting (mandatory for major incidents, optional otherwise).

Knowledge Check

Which of these handling cycles is correct?

Figure A

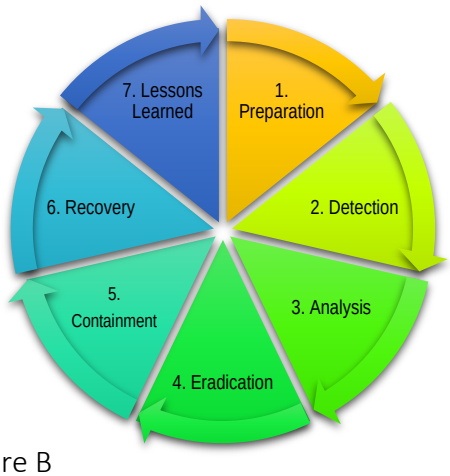

Figure B

Answer: Figure A.

Explanation: Due to the nature of each individual incident and the circumstances in which an incident may occur, it's hard to develop a detailed list of the exact step-by-step handling procedures for each incident. However, following the incident handling cycle ensures the correct steps are taken to resolve the incident and implement controls to prevent reoccurrence.

Roles in Incidents

IT Administrator's Role in Incident Handling

- IT Administrators are most likely to be involved in the Detection, Response, and Resolution phases of the incident handling life cycle.
- Federal agencies are required by law to report incidents involving the PII to the United States Computer Emergency Readiness Team (US-CERT) as soon as possible and without unreasonable delay.
- Know your OpDiv's incident documentation process and incident handling requirements. Incident handling plans are documented to ensure the security incidents are handled efficiently and effectively.

Privacy Incident Response Team

- A privacy incident requires coordination, collaboration, and communication between the Department and the affected OpDiv.
- The Privacy Incident Response Team (PIRT) oversees the response efforts and activities for suspected or confirmed privacy incidents for the Department.
- The PIRT must review any communication, such as a notification letter, before an OpDiv contacts a potentially impacted individual. The OpDiv may provide credit monitoring to the identity theft victim.

Pop-up Window: List of Response Team email addresses.

Name	Email Address
HHS CSIRC	csirc@hhs.gov
ACF	os-irt@hhs.gov
ACL	csirt@acl.hhs.gov
AHRQ	csirt.ahrq@ahrq.hhs.gov
CDC	secops@cdc.gov
CMS	imt@cms.hhs.gov
FDA	csirt@fda.hhs.gov
HRSA	csirt@hrsa.hhs.gov, hrsasoc@hrsa.gov
IHS	csirt@ihs.gov
NIH	csirt@nih.hhs.gov
OIG	csirt@oig.hhs.gov
OS	os-irt@hhs.gov
SAMHSA	infosecurity@samhsa.hhs.gov

Lesson Summary

HHS handles a huge amount of data that constantly attracts cyber adversaries. Federal agencies are required by law to protect the CUI and report incidents that compromise the CUI as soon as they occur. We learned that IT Administrators are involved in several stages within the incident handling process. It's important to know your response procedures, and to act diligently when incidents occur. Each OpDiv has an incident response plan that describes how to respond at the time of incident.

Lesson Quiz

1. PII breaches should be reported to the US-CERT within how much time of their discovery?
   A. One business day
   B. One hour
   C. Three hours
   D. As soon as possible

Answer: B

2. In the Incident Handling Checklist, if more than one host is affected, the recommended action is to repeat some steps for each host. What are those steps?
   A. 1- Analyze the precursors and indicators; 2- Look for correlating information; 3- Contain the incident; 4- Eradicate
   B. 1- Perform research; 2- Acquire, preserve, secure, and document evidence; 3- Contain the incident; 4- Recover from the incident
   C. 1- Look for Correlating information; 2- Contain the incident; 3- Recover from the incident; 4- Create a follow up report
   D. 1- Analyze the precursors and indicators; 2- Look for correlating information; 3- Eradicate the incident; 4- Hold a lessons learned meeting

Answer: A

3. Examples of PHI include:
   A. Name, address, birthdate, SS#, email address
   B. Medical records, diagnosis, treatment, test results
   C. Billing records, research records, referral authorizations
   D. All of the above.

Answer: D.

Section 3 - Conclusion

Training Summary and Final Quiz

Training Wrap Up

At one time, the IT Administrators were only responsible for traditional administrative tasks for the systems they supported. However the responsibility of protecting information assets now falls on the shoulders of the IT Administrators and other IT professionals due to the ever-changing risk environment brought about by the interconnection of information systems.

In all aspects of information protection in the Department, your presence is vital. In the Risk Management Framework, through continuous monitoring, you are the one who detects issues and addresses them; manages user's level access; ensures the performance parameters are optimal and stays vigilant to abnormal usage patterns.

Systems' configuration, successful installation, transfer or change of an information system depend on you to make sure that security measures are all in place. For patch management, you are responsible for maintaining the system components with up-to-date patches, and having data backups ready when you perform system updates.

You also have a major role in contingency planning to develop a plan specific to your information system. This includes making sure that the hardware/software is always up-to-date. In some situations, you may need to modify or change the controls to accommodate HHS missions, so always remember to document your activities.

At the end of the system's lifecycle, you are entrusted with decommissioning the system so that it is formally shut down, and that the media is sanitized (removed, destroyed or retained). It's your responsibility to constantly ensure that your documents and reports are up-to-date; and that the POA&M are remediated before system inspections.

As an IT Administrator, you are in charge of protecting CUI, which includes minimizing and monitoring the access to PII and PHI data. When incidents happen, you will be involved in detecting, responding and resolving the impact. In every stage, never forget to document your process and report the privacy incidents to the right venues.

In your position, it is your responsibility to maintain the security of the Department's information and information systems and assets at all times.

Training Quiz

1. IT Administrators are most likely to be involved in which of the phases of the incident handling life cycle?
   A. Detection
   B. Response
   C. Reporting
   D. All the above

Answer: D.

2. In the event of incident, what are the minimum actions that the IT Administrator can take?
   A. Acquire, preserve, secure and document evidence.
   B. Prioritize action based on the functional and information impacts and recoverability efforts.
   C. Plan for and initiate any necessary corrective actions.
   D. All of the above.

Answer: D.

3. This is a document that every IT system should have to identify, manage, and mitigate weaknesses:
   A. POA&M
   B. Continuous Monitoring
   C. FISMA
   D. Risk Factor

Answer: A.

4. Which of the following is NOT part of the ISCM Control Matrix?
   A. System Security Plan.
   B. Federal Information Process Standards.
   C. Audit Review, Analysis and Reporting.
   D. Security Assessments.

Answer: B.

5. The asterisks that pop up when you type your password in the log in page denote that _____ are implemented:
   A. Common Controls
   B. Hybrid Controls
   C. System-Specific Controls
   D. Risk Factors

Answer: C.

6. The law that was passed to combat waste, fraud, and abuse in health insurance and health care delivery is called:
   A. FISMA
   B. FIPS
   C. HIPAA
   D. NIST

Answer: C.

Training Feedback and Completion

Feedback

We'd love to hear from you! Please provide your feedback so that we can improve as needed.

Feedback Pop-up Window

Welcome to the feedback section of the training! We'd love to hear from you! We cannot do better without your feedback. Once you've completed the training, you will have the opportunity to provide your feedback by sending an email to OIS_Training@hhs.gov. Your feedback is optional, but it is very helpful for the continuous improvement of the training.

Course Completion

Please click the "Course Completion" button upon completion if you are taking this training over the Internet or Intranet. Be sure to print the form and submit to your manager.

Appendixes

Appendix A: Images' Description

HHS ISCM Process in Page 12

Security Control Assessment:

* ISCM Controls
* System Changes
* Ongoing Remediation

Security Status Monitoring:

* Asset Discovery and Management
* Vulnerability Assessment and Management
* Configuration Compliance Management
* Event/Audit Monitoring
* Account Monitoring

Security Status Reporting

* Risk Status
* POA&M
* Metrics

HHS ISCM Implementation Process chart in Page 15

1- Define Process: Action by: HHS

* Strategy
* Goals and objectives

2- Establish Program: Action by: HHS

* Minimum control selections
* Control monitoring frequencies
* Control assessment frequencies
* Control reporting frequencies
* Technical architecture
* Metrics

3- Implementation Process: Action by: OpDiv

* Security status monitoring
* Control assessment
* Security status
* Ongoing authorization

4- Analyze and report: Action by: HHS, OpDiv/StaffDiv

* Data analysis
* Risk decisions
* Incident reporting
* External reporting

5- Respond: Action by: HHS, OpDiv/StaffDiv

* Incident response

6- Review and Update: Action by: HHS

* Program policies and procedures

Appendix B: Acronyms

Do you need help remembering some of the terms from this training?

Pop-up Window: List of acronyms related to this training.

AO	Authoring Officer
ATO	Authority to Operation
CIA	Confidentiality, Integrity, Availability
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GFE	Government Furnished Equipment
HIPAA	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
IS2P	HHS Information Security Plan
ISCM	Information Security Continuous Monitoring
ISP	Information Security Plan
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PHI	Personal Health Information
PII	Personally Identifiable Information
PD	Presidential Directives
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SP	Special Publication
SSP	System Security Plan

Appendix C: References

1. *HHS Information Security and Privacy Policy (IS2P) link: http://intranet.hhs.gov/it/cybersecurity/policies/index.html. Users need to create an account in MAX to be able to read through the policy.*
2. *Federal Information Security Modernization Act (FISMA), 2014: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.*
3. *Cybersecurity framework: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf*
4. *NIST publications: NIST List of Publications*
5. *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*
6. *Risk Management Framework Presentation: http://csrc.nist.gov/groups/SMA/fisma/documents/risk-management-framework-2009.pdf*
7. *Risk Management Framework FAQ: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/select/faq-Select-step2.pdf*
8. *FIPS 199- http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf*
9. *FIPS 200- Minimum Security Requirements for Federal Information and Information Systems: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf*
10. *NIST SP 800-30, Revision 1, Risk Management Guide for Information Technology Systems: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*
11. *NIST SP 800-53: Security and Privacy Controls for Federal Information Security Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*
12. *NIST SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf*
13. *NIST SP 800-88, Guidelines for Media Sanitization: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf*
14. *NIST SP 800-137, Revision 1, Information Security Continuous Monitoring for Federal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf*
15. *Executive Order 13556 -- Controlled Unclassified Information: https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information*
16. *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf*
17. *OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information and NIST SP 800-122 Guide to Protecting the Confidentiality of PII: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf*
18. *Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*
19. *Health Insurance Portability and Accountability Act of 1996 (HIPAA): https://www.hhs.gov/hipaa/for-professionals/index.html*
20. *The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009: https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html*
21. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal*
22. *OMB Circular A-130: https://www.whitehouse.gov/omb/circulars_a130_a130trans4*
23. *E-Government Act of 2002: https://www.archives.gov/about/laws/egov-act-section-207.html*
24. *Clinger-Cohen Act: https://www.gsa.gov/graphics/staffoffices/Clinger.htm*
25. *What health information protected by privacy rules? https://privacyruleandresearch.nih.gov/pr_07.asp*
26. *OMB 14-03: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf*
27. *https://www.mba.org/2015-press-releases/sept/mba-releases-new-white-paper-on-information-security*
28. *https://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343*

Rules of Behavior for Privileged Users v. 3.0

The following *HHS/OpDiv Rules of Behavior (RoB) for Privileged Users* is an addendum to the *Rules of Behavior for General Users* and provides mandatory rules on the appropriate use and handling of HHS/OpDiv information technology (IT) resources for all HH privileged users, including federal employees, interns, contractors, and other staff who possess privileged access to HHS/OpDiv information systems.[1] Privileged users have network accounts with elevated privileges that grant them greater access to IT resources than non-privileged users. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators.[2] The compromise of a privileged user account may expose HHS/OpDiv to a high-level of risk; therefore, privileged user accounts require additional safeguards.

A privileged user is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. System accounts and level of privilege vary dependent upon the role being fulfilled. A privileged user has the potential to compromise the three security objectives of confidentiality, integrity, and availability. Such users include, for example, security personnel or system administrators who are responsible for managing restricted physical locations or shared IT resources and have been granted permissions to create new user accounts, modify user privileges, as well as make system changes. Examples of privileged users include (but are not limited to):

1. Application developer
2. Database administrator
3. Domain administrator
4. Data center operations personnel
5. IT tester/auditor
6. Helpdesk support and computer/system maintenance personnel
7. Network engineer
8. System administrator
9. Security Stewards

Privileged users must read, acknowledge, and adhere to the RoB for Privileged User and any other HHS/OpDiv policy or guidance for privileged users, prior to obtaining access and using HHS/OpDiv information, IT resources and information systems and/or networks in a privileged role. The same signature acknowledgement process followed for the Appendix D, General User RoB, applies to the privileged user accounts. Each OpDiv must maintain a list of privileged users, the privileged accounts those users have access to, the permissions granted to each privileged account, and the authentication technology or combination of technologies required to use each privileged account[3].

[1] Per NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, privileged roles include, for example, key management, network and system administration, database administration, and Web administration.
[2] OMB-16-04 available at Review-Doc-2015-ITOR-315-1.docx (whitehouse.gov), October 30, 2015.
[3] Per NIST White Paper, *Best Practices for Privileged User PIV Authentication,* April 21, 2016, available at https://csrc.nist.gov/publications/detail/white-paper/2016/04/21/best-practices-for-privileged-user-piv-authentication/final.

Following is the RoB for a privileged user.

I understand that as a privileged user, I must:

1. Use privileged user accounts appropriately for their intended purpose and only when required for official duties.
2. Comply with all privileged user responsibilities in accordance with the HHS Policy for Information Security and Privacy Protection (IS2P) and any other applicable HHS and OpDiv policies.
3. Notify system owners immediately when privileged access is no longer required.
4. Properly protect all information, including media, hard copy reports and documentation as well as system information in a manner commensurate with the sensitivity of the information and securely dispose of information and GFE that are no longer needed in accordance with HHS/OpDiv sanitization policies.
5. Report all suspected or confirmed information security incidents and privacy breaches to the OpDiv Helpdesk, HHS/OpDiv CSIRC, or OpDiv CSIRT as soon as possible, without unreasonable delay and no later than within ***one (1) hour*** of occurrence/discovery.
6. Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a privileged user, I must **not:**

1. Share privileged user account(s), password(s)/passcode(s)/PIV PINs, and other login credentials, including to other system administrators.
2. Conduct official HHS/OpDiv business using personal email or personal online storage account.
3. Use privileged user access to log into any system for non-elevated duties.
4. Install, modify, or remove any system hardware or software unless it is part of my job duties and the appropriate approvals have been obtained or with official written approval.
5. Access the internet for any reason while using my privileged account. This includes downloading of files (including patches or updates), etc.
6. Remove or destroy system audit logs or any other security, event log information unless authorized by appropriate official(s) in writing.
7. Tamper with audit logs of any kind. Note: In some cases, tampering can be considered evidence and can be a criminal offense punishable by fines and possible imprisonment.
8. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes.
9. Introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into HHS/OpDiv information systems or networks.
10. Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses.
11. Use privileged user account(s) for day-to-day communications and other non-privileged transactions and activities.
12. Elevate the privileges of any user without prior approval from the system owner.
13. Use privileged access to circumvent HHS/OpDiv policies or security controls.

14. Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals.
15. Use a privileged user account for web access except in support of administrative related activities.
16. Use any unknown website(s) which may be infected with malware and responding to phishing emails. If I use, I will report to OpDiv Helpdesk, HHS/OpDiv CSIRC, or OpDiv CSIRT as soon as possible, without unreasonable delay and no later than within ***one (1) hour*** of occurrence/discovery.
17. Use any file sharing program without HHS/OpDiv's permission.
18. Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner.
19. Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS/OpDiv information:
    - Antivirus software with the latest updates
    - Anti-spyware and personal firewalls
    - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access
    - Approved encryption to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

SIGNATURE

I have read the above *Rules of Behavior (RoB) for Privileged User*s and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or HHS/OpDiv information security policies and standards may result in disciplinary action and that these actions may include reprimand, suspensive of access privileges, revocation of access to federal information, information systems, and/or facilities, deactivation of accounts, suspension without pay, monetary fines, termination of employment; removal or debarment from work on federal contracts or projects; criminal charges that may result in imprisonment. I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing official(s).

User's Name: _____

(Print)

User's Signature: _____

Date Signed: _____