

**Centers for Medicare & Medicaid Services**

**Information Security and Privacy Group**

Information System Security Officer Guide

Version 1.0

  June 17, 2020

**INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:** This information has not been publicly disclosed and may be privileged and confidential.  It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information.  Unauthorized disclosure may result in prosecution to the full extent of the law.Document Change History

The “Record of Changes” table below should be used to capture changes when updating the document. All columns are mandatory.

| **Version Number** | **Date** | **Author/Owner Name** | **Description of Change** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Chapter 1: Introduction 8](#_Toc41482498)

[1. Purpose 8](#_Toc41482499)

[2. Scope 8](#_Toc41482500)

[3. Navigating This Guide 8](#_Toc41482501)

[4. A Note to New ISSOs 8](#_Toc41482502)

[Chapter 2: The CMS Information Security and Privacy Program 9](#_Toc41482503)

[1. Introduction 9](#_Toc41482504)

[2. Program Overview 9](#_Toc41482505)

[3. CISO/ISPG Organization 10](#_Toc41482506)

[1. Office of the CISO 10](#_Toc41482507)

[2. Information Security and Privacy Group (ISPG) 11](#_Toc41482508)

[4. The Portfolio Team 13](#_Toc41482509)

[1. Program Executive, Information System Owner, Business Owner, and ISSO 13](#_Toc41482510)

[2. Cyber Risk Advisor (CRA) 13](#_Toc41482511)

[3. Data Guardian 13](#_Toc41482512)

[4. Privacy Advisor 13](#_Toc41482513)

[Chapter 3: The CMS ISSO 15](#_Toc41482514)

[1. Introduction 15](#_Toc41482515)

[2. The ISSO Role 15](#_Toc41482516)

[3. Business Knowledge 15](#_Toc41482517)

[4. ISSO Essentials 15](#_Toc41482518)

[5. Duties and Responsibilities 15](#_Toc41482519)

[6. ISSO Designation and appointment letter 16](#_Toc41482520)

[7. Goals for The ISSO’s First Year 16](#_Toc41482521)

[Chapter 4: ISSO Actions 18](#_Toc41482522)

[1. *Sidebar*: Key Tools 18](#_Toc41482523)

[1. CFACTS 18](#_Toc41482524)

[2. CMS Acceptable Risk Safeguards 19](#_Toc41482525)

[2. Security Impact Assessment (SIA) 19](#_Toc41482526)

[3. System Categorization 20](#_Toc41482527)

[4. Determine the Authorization Boundary 20](#_Toc41482528)

[5. *Sidebar*: High Value Assets (HVA) 20](#_Toc41482529)

[6. Allocate controls 21](#_Toc41482530)

[1. System Specific Controls 21](#_Toc41482531)

[2. Inherited Controls 21](#_Toc41482532)

[3. Non-Mandatory Controls 21](#_Toc41482533)

[7. Implement Security Controls 22](#_Toc41482534)

[8. *Sidebar:* Develop System Documentation 22](#_Toc41482535)

[1. System Security Plan (SSP) 22](#_Toc41482536)

[2. Information System Risk Assessment (ISRA) 22](#_Toc41482537)

[3. Privacy Impact Assessment (PIA) 22](#_Toc41482538)

[4. Third-Party Websites and Applications 23](#_Toc41482539)

[5. Privacy Threshold Analysis 24](#_Toc41482540)

[9. *Sidebar*: Contingency Planning 24](#_Toc41482541)

[1. Contingency Plan (CP) Document 25](#_Toc41482542)

[2. CP Plan Exercise 25](#_Toc41482543)

[3. After Action 25](#_Toc41482544)

[4. CP Re-certification 25](#_Toc41482545)

[10. Assess Controls 26](#_Toc41482546)

[1. Security Controls Assessment. (SCA) 26](#_Toc41482547)

[2. Adaptive Capabilities Testing (ACT) 26](#_Toc41482548)

[3. Penetration Testing 27](#_Toc41482549)

[4. Security Assessment Report (SAR) and CAAT File 27](#_Toc41482550)

[11. Plan of Action and Milestones (POA&M) Management 27](#_Toc41482551)

[1. Methods of risk mitigation 27](#_Toc41482552)

[2. Reports 29](#_Toc41482553)

[3. POA&M Closing Requirements 29](#_Toc41482554)

[12. Authorize the System 29](#_Toc41482555)

[13. Continuous Monitoring 30](#_Toc41482556)

[14. *Sidebar*: Managing Security Incidents 30](#_Toc41482557)

[15. ISSO Recurring Tasks 30](#_Toc41482558)

[1. Ongoing Activities 30](#_Toc41482559)

[2. ISSO Annual Activities 31](#_Toc41482560)

[3. As Required Activities 31](#_Toc41482561)

[Chapter 5: ISSO Tools 32](#_Toc41482562)

[1. ISSO Welcome Packet 32](#_Toc41482563)

[2. ISSO Mentoring 32](#_Toc41482564)

[3. The “ISSO Toolbox” 32](#_Toc41482565)

[1. CISO Mailbox 33](#_Toc41482566)

[2. CMS Information Security and Privacy Website 33](#_Toc41482567)

[3. CMS ISSO Framework 33](#_Toc41482568)

[4. ISSO SharePoint Site 34](#_Toc41482569)

[5. ISSO Forum 34](#_Toc41482570)

[6. ISSO Journal 35](#_Toc41482571)

[Chapter 6: Important Reference Information 36](#_Toc41482572)

[1. HHS Information Security and Privacy Policy (HHS IS2P) 36](#_Toc41482573)

[2. CMS Information Security and Privacy Policy (CMS IS2P2) 36](#_Toc41482574)

[3. Information Security and Privacy Library 36](#_Toc41482575)

[4. CMS Risk Management Handbooks 36](#_Toc41482576)

[5. NIST Special Publications 37](#_Toc41482577)

[6. CMS Information Security Contract Clause/Provision 37](#_Toc41482578)

[7. Security in the System Development Lifecycle (SDLC) 37](#_Toc41482579)

[8. Spotlight 37](#_Toc41482580)

[9. Enterprise User Administration 38](#_Toc41482581)

[10. OMB Memoranda 38](#_Toc41482582)

[11. OMB Circulars 38](#_Toc41482583)

[Chapter 7: Training 39](#_Toc41482584)

[1. Introduction 39](#_Toc41482585)

[2. Getting Started 39](#_Toc41482586)

[3. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Overview 39](#_Toc41482587)

[4. Sources 40](#_Toc41482588)

[5. Recommended Training Sources, by Experience 40](#_Toc41482589)

[1. Recommended ISSO Training Courses – Basic 40](#_Toc41482590)

[2. Recommended ISSO Training Courses – Intermediate 41](#_Toc41482591)

[3. Recommended ISSO Training Courses – Advanced 42](#_Toc41482592)

[Appendix A: Cybersecurity Certifications 44](#_Toc41482593)

[1. Federal IT Security Professional Certification (FITSP) 44](#_Toc41482594)

[2. CompTIA A+ Certification 45](#_Toc41482595)

[3. CompTIA Network+ 45](#_Toc41482596)

[4. CompTIA Security+ 45](#_Toc41482597)

[5. (ISC)2 System Security Certified Practitioner (SSCP) 45](#_Toc41482598)

[6. SANS GIAC Information Security Fundamentals Certification (GISF) 45](#_Toc41482599)

[7. Microsoft Certification Programs 46](#_Toc41482600)

[8. ITILTM Certification 46](#_Toc41482601)

[1. Foundation 46](#_Toc41482602)

[2. Intermediate 46](#_Toc41482603)

[3. Managing across the Lifecycle 47](#_Toc41482604)

[4. Expert 47](#_Toc41482605)

[9. Advanced Certifications 47](#_Toc41482606)

[1. CompTIA Advanced Security Practitioner (CASP) 47](#_Toc41482607)

[2. Certified Information Systems Security Professional (CISSP) 47](#_Toc41482608)

[3. SANS GIAC Security Certifications 48](#_Toc41482609)

[4. Cisco Certified Network Associate (CCNA) 48](#_Toc41482610)

[10. In Summary 48](#_Toc41482611)

[Appendix B: Security Certification Ladder 49](#_Toc41482612)

[Entry Level 49](#_Toc41482613)

[Associate Level 49](#_Toc41482614)

[Professional Level 49](#_Toc41482615)

[Expert Level 50](#_Toc41482616)

[Architect Level 50](#_Toc41482617)

[Security Certification Path 50](#_Toc41482618)

[CompTIA Security+ 50](#_Toc41482619)

[(ISC)² Systems Security Certified Practitioner (SSCP) 50](#_Toc41482620)

[SANS GIAC Information Security Fundamentals Certification (GISF) 51](#_Toc41482621)

[CompTIA Advanced Security Practitioner (CASP) 51](#_Toc41482622)

[(ISC)² Certified Information Systems Security Professional (CISSP) 51](#_Toc41482623)

[SANS GIAC Security Certifications 51](#_Toc41482624)

[Qualified Information Security Professional Certification 51](#_Toc41482625)

[Appendix C: Career Self-Assessment 52](#_Toc41482626)

[Appendix D: Risk Management Handbook Quick Guide 53](#_Toc41482627)

# Chapter 1: Introduction

## Purpose

This guide provides practical guidance to the Centers for Medicare & Medicaid Services (CMS) Information System Security Officers (ISSO)s when performing their necessary tasks. It lists and explains the responsibilities, duties, tasks, resources, and organizational relationships needed for an ISSO to be successful.

## Scope

This guide is applicable to CMS (Federal) ISSOs, Contractor ISSOs, and contract security support individuals. Business Owners and their staff will find parts of this document useful, particularly when appointing new ISSOs or gaining a better understanding of ISSO tasks.

## Navigating This Guide

The guide is comprised of seven chapters, each providing information to specific audiences:

1. Chapters Two and Three provide information that is useful to both the ISSO and the Business Owner, and others as appropriate. The CMS Information Security Program is laid out, including all of the key CMS participants.
2. Chapter Four is the “meat and potatoes” for ISSOs. It gives specific information about the many tasks to perform as an ISSO. This will be the most frequently-used section of this guide for ISSOs.
3. Chapter Five introduces most of the many tools that are available to help ISSOs do their jobs effectively.
4. Chapter Six introduces references that the ISSO will find useful.
5. Chapter Seven introduces training requirements and opportunities for the ISSO. It is followed by appendices that put training and career paths in perspective for ISSOs.

## A Note to New ISSOs

You will find that there are many resources available to help you perform your duties successfully. This guide will help you understand what and where they are, and how to use them. The actions that you must take as an ISSO are presented in Section Four. This will provide you a good start; you will find that you must move to the references that are provided to get a complete understanding of your tasks. Think of this guide as an annotated table of contents to being an ISSO.

Finally, ***welcome***! You are part of an important and thriving community at CMS. We encourage you to participate in functions such as the ISSO Forum, write for the ISSO Journal, and attend special presentations. Also, if you feel lost, don’t forget the **ISSO Mentorship Program**. This program is very easy to participate in, and may help you get the context and contacts that you need to begin your career. Send email to [isso@cms.hhs.gov](mailto:isso@cms.hhs.gov) for information.

# Chapter 2: The CMS Information Security and Privacy Program

## Introduction

This chapter provides an overview of CMS’ organization for security and privacy, who the main actors are, the main components, and their functions.

## Program Overview

The CMS information security and privacy disciplines are integrated into a single program called the Information Security and Privacy Program. The CMS Chief Information Security Officer (CISO) and Senior Official for Privacy (SOP) are responsible for managing this program.

Security relates to the tasks associated with ensuring the confidentiality, integrity and availability of CMS systems and sensitive information such as Beneficiary Information. These tasks include:

* Ensuring that policies, standards and guidelines are in place that meet organizational requirements while being implementable,
* Organizing and overseeing periodic assessment and authority to operate (ATO) activities, and
* Ensuring that there are necessary enterprise-level information security capabilities and services in place to protect CMS systems.

Privacy policies apply to CMS programs and activities at their inception, even before information systems are identified or defined. Business Owners (BO) must be engaged at the outset to identify privacy requirements, privacy compliance documentation, and privacy contract requirements prior to system development. Privacy policies also apply to the collection, creation, use, disclosure, and retention of information that identifies an individual in electronic or physical form. It is CMS’s responsibility to protect the privacy interests of individuals and it applies to all types of information, regardless of its form. All CMS standards, regulations, directives, practices, and procedures clearly state that all forms of information must be protected. It is the responsibility of the ISSO to coordinate with the Data Guardian, Information System Owner (ISO), BO, Privacy Advisor, and Cyber Risk Advisor (CRA) to meet all collection, creation, use, dissemination, retention, and maintenance requirements for Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI) in accordance with the Privacy Act, E-Government Act, and all applicable guidance.

The figure below depicts the interrelationship between security and privacy, both of which are vital to CMS operations.

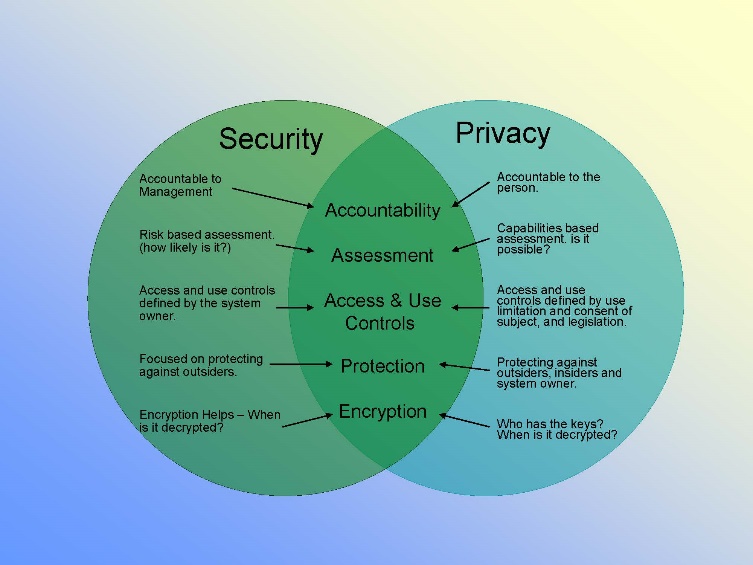


Figure 1 Security and Privacy Interrelationship

## CISO/ISPG Organization

### Office of the CISO

Per the CMS Information System Security and Privacy Policy (IS2P2), Version 2.0, the CISO carries out the CIO’s information security responsibilities under federal requirements in conjunction with the SOP. The responsibilities of the CISO include, but are not limited to, the following:

* Define information security and privacy control requirements through the CMS Acceptable Risk Safeguards (ARS)and standards, requirements, directives, practices, and procedures through the Risk Management Handbook (RMH);
* Publish CISO Directives as required to augment existing policy;
* Review any requested waivers and deviations from policy and provide recommendations to the Authorizing Official (AO) for risk acceptance;
* Serve as the security official who is responsible for the development and implementation of the policies and procedures that are required by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
* Delegate the authority to approve system configuration deviations to the CRA and ISSO, where appropriate;
* Ensure CMS-wide implementation of the Department of Health and Human Services (HHS) and CMS information security and privacy capabilities, policies, and procedures;
* Lead the investigation and resolution of information security and privacy incidents and breaches across CMS;
* Define and oversee the goals and requirements of Agency Security Operations;
* Coordinate incident response and threat information sharing with the HHS Computer Security Incident Response Center (CSIRC) and/or HHS Privacy Incident Response Team (PIRT), as appropriate;
* Ensure the information security continuous monitoring (ISCM) capabilities accomplish the goals identified in the ISCM strategy;
* Approve the appointment of the ISSO by the Program Executive;
* Approve the independent security control assessment deliverables;
* Coordinate with the CIO, SOP, Data Guardian, ISSO, and Website Owner/Administrator to ensure compliance with control family requirements on website usage, web measurement and customization technologies, and third-party websites and applications, and
* Authorize the immediate disconnection or suspension of any interconnection by coordinating with the SOP and the CCIC Director to (1) disconnect or suspend interconnections and (2) ensure interconnections remain disconnected or suspended until the AO orders reconnection.

### Information Security and Privacy Group (ISPG)

ISPG consists of three separate divisions, each of which is responsible for functional area(s) within the CMS security and privacy domain.

#### Security and Privacy Policy and Governance

The policy and governance functional area develops and updates the information security and privacy policies, standards, requirements, directives, practices, and procedures. Responsibilities include developing, implementing, and disseminating this Policy to align with the HHS policies, federal legislation, and best practices.

#### Security and Privacy Compliance

The risk management and compliance functional area oversees Security Assessment and Authorization (SA&A), Federal Information Security Modernization Act (FISMA) reporting, and other external audits. Responsibilities include developing and updating risk management and compliance processes and procedures to align with HHS policies, federal legislation, and best practices.

The awareness and training functional area provides awareness training and role-based training (RBT) for all CMS stakeholders. Responsibilities include developing curriculum, delivering training, tracking training status, and reporting.

#### Enterprise Information Security Capabilities and Services-CMS Cybersecurity Integration Center (CCIC)

##### **Background**

CMS established the CMS Cybersecurity Integration Center (CCIC) to support CMS’s mission in protecting the sensitive and critical information that is processed, stored, and transmitted through its complex information technology infrastructure (IT). To support new Acceptable Risk Safeguards (ARS) requirements, CMS requires the use of diverse IT components and platforms to ensure that the confidentiality, integrity, and availability of its information systems are protected adequately. Utilizing these IT components and platforms, the CCIC will provide enterprise-wide situational awareness and near real-time risk management that will support aggregated monitoring of security events across all datacenters that host CMS information systems. All requirements must be implemented effectively in order for the CCIC to assist and or mange privacy and operational technical security risks.

##### **CCIC Overview**

The CCIC supports and provides a variety of enterprise-level information security capabilities and services for CMS through:

* Maintaining an independent and enterprise-wide information security operations perspective;
* Centrally coordinating CMS enterprise information security operations;
* Centrally coordinating and disseminating information security and privacy threat intelligence applicable to CMS, and
* Providing integration requirements for implementing CCIC technical requirements to ensure a more fully integrated information security environment for the entire enterprise.

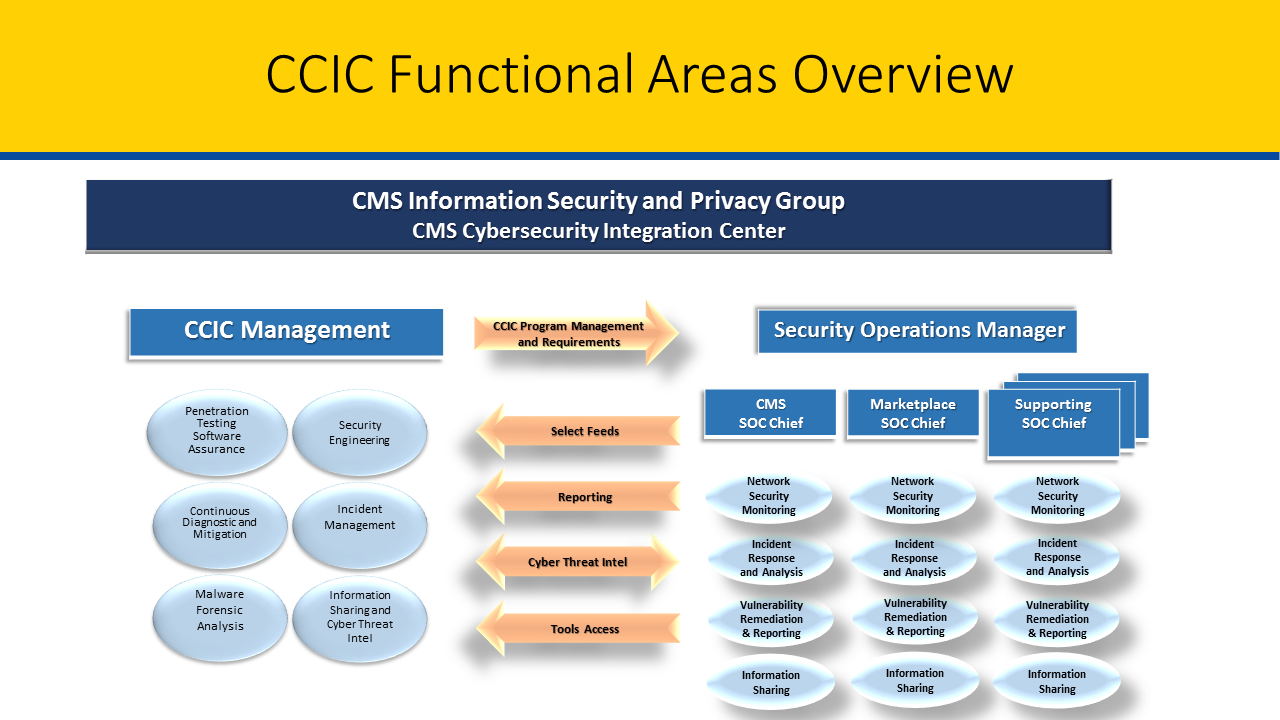


Figure 2 CCIC Functional Areas Overview

The CCIC is not a replacement for, nor is it intended to remove the requirement for a CMS datacenter to have its own security policy, security operations personnel, and security procedures. The CCIC extends the defense-in-depth strategy by providing an additional layer that provides monitoring, response, and notification across the entirety of CMS. This additional layer augments and enhances the security controls and capabilities for information systems hosted at a CMS datacenter.

It is important to note that a CMS system developer/maintainer (SD/M) is expected to maintain responsibility for appropriately staffing and implementing its information security and privacy program to meet CMS requirements. The CCIC can provide assistance in formulating or providing a capability to meet these requirements, but only in an advisory role on a case by case basis.

The cyber threat and incident handling functional area are contained within CCIC and support CMS’s cyber threat intelligence, information sharing, and incident handling, including breach response. Responsibilities include developing, updating, and disseminating processes and procedures to coordinate information sharing and incidents across CMS.

The continuity of operations functional area provides plans and procedures to ensure continuity of operations for information systems that support CMS operations and assets. Responsibilities include developing processes and procedures for system contingency planning, disaster recovery, and participation in federal continuity exercises.

## The Portfolio Team

### Program Executive, Information System Owner, Business Owner, and ISSO

The Program Executive, ISO, BO, and ISSO work together to take full responsibility for implementing the required security and privacy controls and managing the cybersecurity and privacy risk posture for each system.

The Program Executive must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A, Section 20, Program Executive.

The ISO must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A, Section 21, System Owner.

The BO must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A, Section 22, Data Owner/BO in coordination with the Data Guardian.

The ISSO may be either a federal government employee or a contractor and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A, Section 19, ISSO. The ISSO must ensure the duties of the Security Control Assessor and Contingency Planning Coordinator are completed as described in the HHS IS2P Appendix A, Sections 18 and 24 and elaborated upon in this section. (5.1)

### Cyber Risk Advisor (CRA)

The CRA must be an agency official (federal government employee) and a member of ISPG. The CRA facilitates and oversees the completion of all federal cybersecurity and privacy requirements. They act as the SME in all areas of the CMS Risk Management Framework (RMF), and evaluate, maintain, and communicate the risk posture of each FISMA system to executive leadership and make risk-based recommendations to the Authorizing Official.

The CRA supports the CMS stakeholders in ensuring that all requirements specified by the Acceptable Risk Safeguards (ARS) and the procedures and standards of the Risk Management Handbook (RMH) are implemented and enforced.

They also coordinate with the Data Guardian, ISO, Business Owner, and ISSO to identify the types of information processed, assign the appropriate security categorizations to the information systems, determine the privacy impacts, and manage information security and privacy risk. (5.2)

### Data Guardian

The Data Guardian coordinates CMS Program activities involving beneficiary and other types of consumer information that require privacy protections. The Data Guardian must be an agency official (federal government employee) and must fulfill shared responsibilities with the CMS BO identified in the HHS IS2P Appendix A, Section 22, Data Owner/Business Owner. (5.3)

### Privacy Advisor

The Privacy Advisor is a member of ISPG who provides privacy-related expertise to help the team identify and manage privacy risk. The Privacy Advisor is an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 16, OpDiv Privacy Act Contact. These include:

* Serving as a POC for issues related to the *Privacy Act*;
* Coordinating with the SOP on the development, publishing, and maintenance of System of Records Notices (SORN)s;
* Supporting the SOP and CISO in completing required *Privacy Act* reviews, as defined by OMB Circular A-130; and
* Supporting completion of the FISMA and Privacy Management Report for submission to the Department. (5.4)

# Chapter 3: The CMS ISSO

## Introduction

This chapter details the framework for the CMS ISSO program. It provides a high level understanding of ISSO essentials, followed by a more detailed listing of specific responsibilities. The section relating to the ISSO Authorization Letter process may be helpful to the BO. The final section is provided to give ISSOs a feel for how their responsibilities are carried out, when, and under what circumstances. It provides a good snapshot of activities that an ISSO must perform, and provides context for actions that are described further in Chapter Four.

## The ISSO Role

The ISSO role at CMS is a formally appointed position and may be filled by either a federal government employee or a contractor. They must fulfill all of the responsibilities identified in the CMS IS2P2 and HHS IS2P Appendix A, Section 19, ISSO. The ISSO must ensure the duties of the Security Control Assessor and Contingency Planning Coordinator are completed as described in the HHS IS2P Appendix A, Sections 18 and 24.

## Business Knowledge

The goal of every ISSO should be to support the BO to securely provide the service intended by the system. To help accomplish this goal, the prospective ISSOs should know and understand their component’s business processes and how the system supports that business. This knowledge is critically applied during the construction and testing of the system’s contingency plan. Information security is a means to an end and not the end in itself. In the public sector, information security is secondary to the agency's services provided to its constancy. We, as security professionals, must not lose sight of these goals and objectives.

## ISSO Essentials

The goal of information security and privacy is to help the CMS BO provide a service in a manner that is both demonstrably secure and that safeguards sensitive beneficiary information. To be successful, at a minimum, the ISSO needs to know and understand the following:

* Mission and business functions of their component;
* How the system supports the component’s mission;
* System details, including:
  + Architecture
  + System components (hardware, software, peripherals, etc.)
  + Location of each system component
  + Data flow
  + Interconnections (internal and external)
  + Security categorization
  + Security requirements
  + Configuration management processes and procedures;
* Users (How many, location, etc.), and
* Key personnel by name.

## Duties and Responsibilities

The responsibilities of the CMS ISSO include but are not limited to the following:

* Complete the security categorization for the FISMA system using the CFACTS tool;
* Complete and maintain the System Security Plan using the CFACTS tool;
* Ensure Security Controls Assessment (SCA) (also known as Adaptive Capabilities Testing (ACT)), and Penetration Tests have been scheduled and completed in a timely manner;
* Develop, document and maintain an inventory of hardware and software components within the FISMA system’s authorization boundary;
* Coordinate the development of a Contingency Plan and ensure the plan is tested and maintained accordingly;
* Maintain primary responsibility for the actions and activities associated with the FISMA system receiving and maintaining an Authority to Operate (ATO);
* Coordinate with the ISO, BO, and CRA to manage information security and privacy risk;
* Monitor and update all POA&Ms in accordance with current requirements and instruction;
* Submit recommendations to the CRA for system configuration deviations from the required baseline;
* Identify the information security and privacy controls provided by the applicable infrastructure that are common controls for information systems;
* Coordinate with the, ISO, BO, and CRA to meet all collection, creation, use, dissemination, retention, and maintenance requirements for PII, PHI, and FTI in accordance with the Privacy Act, E-Government Act, and all other applicable guidance;
* Coordinate with the BO, Contracting Officer, ISO, and CISO to ensure that all requirements specified by the ARS and the RMH are implemented and enforced for applicable information and information systems;
* Report and manage IT Security and Privacy Incidents in accordance to the RMH and other applicable federal guidance.

## ISSO Designation and appointment letter

The CMS Program Executive in coordination with the Data Guardian, ISO, and Business Owner, is responsible for nominating appropriately qualified ISSO appointees, as defined under FISMA[[1]](#footnote-2), to the CISO for approval.

The nominated ISSO, by signing the appointment letter, agrees to maintain the appropriate operational security posture of the information system by fulfilling all of the responsibilities identified in the CMS Information Systems Security and Privacy Policy (CMS IS2P2) Section 3.4.7, Information Systems Security Officer; and HHS Information System Security and Privacy Policy Appendix A, Section 19. A subset of the ISSO’s duties and responsibilities is contained in the letter.

ISSO letters must be updated whenever a change occurs. The designated ISSO should be consistently identified in three sources: the ISSO letter, the SSP and in CFACTS. The signed appointment letter should be given to the appropriate CRA for further action. It is the responsibility of the CRA to upload the letter to CFACTS.[[2]](#footnote-3)

## Goals for The ISSO’s First Year

During an ISSO’s first year, the new ISSO should:

* Learn the security planning and administrative security procedures for systems that process sensitive information such as PHI, PII, and classified and national intelligence data.
* Understand the implementation and enforcement of CMS’ Information System Security and Privacy policies and practices
* Know the concerns and requirements that determine the administration and management of physical, system, and data access controls based on the sensitivity of the data processed and the corresponding authorization requirements
* Learn the identification, analysis, assessment and evaluation of information system threats and vulnerabilities and their impact on their component’s critical information infrastructures
* Be able to identify management, technical, personnel, operational and physical security controls
* Understand any additional critical areas of knowledge related to your system.

# Chapter 4: ISSO Actions

This chapter introduces the largely sequential actions that you must understand and perform as an ISSO from the very beginning of your system’s development. Each activity is described, along with pertinent references.

The two major sources which describe the sequence of actions that you need to understand and perform as an ISSO are described in System Development Lifecycle Activities (SDLCs) and frameworks. The two major SDLCs for CMS systems are the **eXpedited Life Cycle (XL**C) and the **Target Life Cycle (TLC)**. NIST has described a **Risk Management Framework (RMF)** which further describes necessary activities.

There are some topics that are important to understand, but are not necessarily part of the sequence of events from system initiation to disposition. Rather than list these topics at the end of this chapter, they are interspersed within the sequential list of activities. They will still be numbered (to ensure that they appear in the Table of Contents), but will be prefaced as “***Sidebar***” actions. Accordingly, the first sequential action that you must understand begins with “Security Impact Assessments”, after the discussion of Key Tools.

## *Sidebar*: Key Tools

Actions that you will perform most frequently will involve the CMS Federal Information Security Management Act (FISMA) Controls Tracking System (CFACTS) tool and the Acceptable Risk Safeguards (ARS). Before we talk about the actions that you need to take across your role as ISSO, we will start with a discussion of these necessary tools. Other key references are described in later chapters.

### CFACTS

CFACTS is the CMS Federal Information Security Management Act (FISMA) Controls Tracking System. CFACTS provides for the electronic management of all cybersecurity relevant information for the CMS FISMA systems throughout the entire system lifecycle. CFACTS is a Web-based application accessible to Users based on roles assigned within the application. The access to the application will be governed by CMS standard ID and password rules.

The Assessment & Authorization (A&A) workspace, allows the User to securely maintain and document compliance for the CMS component’s assigned information systems. The purpose of the A&A workspace is twofold: it first defines what hardware, software, location and data the component contains; and second, it defines and manages the relationship between the data assets and the component hierarchy, stakeholders and enterprise infrastructure.

A User’s Manual[[3]](#footnote-4) is available that instructs the User in the following elements of the CFACTS Application:

* How to request access
* Method of access
* How to log in
* How to navigate the various screens
* How to run reports
* How to upload documents
* Where to find help

### CMS Acceptable Risk Safeguards

#### Overview

The CMS Information Security Acceptable Risk Safeguards (ARS)[[4]](#footnote-5) defines information security and privacy control requirements and includes additional, detailed policy traceability statements within each control description. The ARS provides guidance on customizing (tailoring) controls and enhancements for specific types of missions/business functions, technologies, or environments of operation. Users of the ARS may tailor specific mandatory controls as well as most of the non-mandatory and unselected controls.

#### Intent

The goal of the ARS is to define a baseline of minimum information security and privacy assurance controls. The controls are based on both internal CMS governance documents and laws, regulations, and other authorities created by institutions external to CMS.

Protecting and ensuring the confidentiality, integrity, and availability for all of CMS’ information and information systems is the primary purpose of the information security and privacy assurance program. The ARS complies with the CMS IS2P2 by providing a defense-in-depth security structure along with a least-privilege, need-to-know basis for all information access.

#### Controls

Incorporating controls cataloged in the ARS will ensure that CMS and CMS contractor systems meet a minimum level of information security and privacy assurance. CMS systems are also subject to technical security protections defined under CMS’ other governance documents (e.g., the CMS Technical Reference Architecture (TRA), applicable TRA Supplements, and the CMS Expedited Life Cycle (XLC)). These documents, managed under the Office of the CMS CIO, describe architecture and lifecycle standards required of CMS systems.

The controls within the ARS are not intended to be an all-inclusive list of information security and privacy requirements nor are they intended to replace a Business Owner’s due diligence to incorporate additional controls to mitigate risk. The ARS controls are the minimum-security and privacy requirements to be considered and employed where applicable throughout the risk management process and the CMS XLC.

#### Responsibilities

Business Owners must review both the non-mandatory (CMS recommended) controls and enhancements listed in the ARS and controls and enhancements under NIST SP 800-53 that were not selected (i.e., those that CMS did not pre-select for inclusion into the ARS as mandatory controls and enhancements, or that CMS selected for inclusion in the ARS but only as non-mandatory controls and enhancements) to determine if any of the controls and/or enhancements would assist in reducing risks to the system.

## Security Impact Assessment (SIA)[[5]](#footnote-6)

The Security Impact Assessment is the process that you will use initially for your new system and *every time* a new change to the system is proposed.

When you have completed this process, you will be able to provide substantive recommendations to your Business Owner on the impact of any proposed change(s). The impact may be small, or it may rise to the level of a new ATO process.

Note: SIAs are frequently thought of as documents. Remember that SIA is a *process*. Based on the complexity and extent of the process, a completed form may help better describe the security impact, as well as necessary actions to take. The actual CMS/FISMA requirement noted in ARS Control CM-4 requires “*Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) to conduct security impact analyses*.” It is up to you and your Business Owner/organization to determine the level to which you document your assessment.

## System Categorization[[6]](#footnote-7)

Your FISMA system has different security controls based on the sensitivity of the information contained in or processed by your system. **Categorization** takes place within CFACTS. You enter the appropriate area and select the type of information that will be processed. The system categorization will be suggested automatically and noted as “Low”, “Moderate”, or “High”. If necessary, the categorization may be manually overridden; your CRA will have to help with this. In practice this seldom happens. This system categorization will have a variety of uses. Most importantly you will need to have this information to determine which controls to allocate for your system.

**Key Point**. Although this process sounds like it will only be done once for your FISMA system, you may have to repeat it if a proposed change includes access or storage of different types of data. Your completed SIA will guide your actions.

## Determine the Authorization Boundary[[7]](#footnote-8)

Another major initial task is to determine the system’s **Authorization Boundary**. NIST’s definition of authorization boundary is… “All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected”. One practical way of determining the system’s authorization boundary is to ask whether a particular component can be changed by one’s system team, or if another team has to make updates or changes. If your team can make the change or configuration, chances are that the component falls within your authorization boundary. As with system categorization, the authorization boundary is usually determined at the outset of system development. It may expand or contract based on changes to the system over its lifecycle.

## *Sidebar*: High Value Assets (HVA)[[8]](#footnote-9)

The *HHS HVA Program Policy* defines HVAs as: “Assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States’ national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people*.”*

The practical impact of this program is that, if your FISMA system is defined as an HVA, it will face additional security requirements from DHS and HHS, which may impact the continuity operations and assessments of the system.

## Allocate controls

Once a system has been categorized, the ISSO has the information necessary to select controls, or **allocate** them. The process is largely automatic, and is well-described in Risk Management Handbook (RMH) *Chapter 12: Security and Privacy Planning,* Section 3.1.6. Selected controls are allocated for Low, Moderate, or High systems based on system categorization. The mechanics are described very well in the *CFACTS User Manual, Version 4.5*, Section 4.5.1. Some general control types are worth describing.

### System Specific Controls

These are controls that your system “owns”. If you are running on hardware that you are responsible for, there are system specific controls for it. If your system is an application, or **Major Application,** the system specific controls are those controls that your developers and administrators configure and maintain.

### Inherited Controls[[9]](#footnote-10)

In many cases your system uses components provided by other FISMA systems. In the example noted above about hardware, what if your system is housed on hardware administered by others? This is not just a possibility. In most cases major applications run within a separate data center. Certainly this is the case for systems housed in the AWS Cloud. In these instances, the data center (or other entity) that houses your system will most likely take care of some of the controls for your system. In this case your system will be able to **inherit controls**. If the providing system completely takes care of a control, it is called a **common, or fully inherited control** If the providing system takes care of part of a control, and relies on your system to take care of the rest of the control, it is called a **hybrid control**.

Understanding which controls your team must address and which controls are available through full or partial inheritance will help you understand how to document your security control compliance, the next step in the cycle.

### Non-Mandatory Controls[[10]](#footnote-11)

ARS 3.1 introduced a new category of control called **non-mandatory controls.** These controls are described as controls that “…may offer additional protection that should be considered by the Business Owner as part of risk management.”

**Note:** *The practical impact to you as an ISSO is that it is your responsibility to evaluate each non-mandatory control and coordinate with your Business Owner to determine whether the non-mandatory control is germane to your system. If it is applicable, treat it as you would treat any other control. If you determine, and your Business Owner agrees, that the non-mandatory control is not necessary, document the fact that you and your Business Owner have decided that the control is not germane. Do not ignore the control out of hand.*

## Implement Security Controls[[11]](#footnote-12)

It is your responsibility as your system’s security and privacy Subject Matter Expert to make sure that your Business Owner, system developers, and system administrators understand the controls that must be in place for your system to be “secure” to CMS standards. Once these controls have been implemented, they need to be documented within CFACTS.

**Note:** *All security controls that have been allocated for your system must have some comment. Non-mandatory controls that have been determined not to be mandatory for your system must have notation describing the deliberative process with which the determination was made. Even fully inherited controls should have a notation that the control is fully inherited.*

## *Sidebar:* Develop System Documentation[[12]](#footnote-13)

Prominent documents are important to understanding the security posture of your FISMA system. CFACTS can helps with this process by automatically generating some of the documents, such as the System Security Plan. Other documents are found within CFACTS, such as System Categorization. Others, such as the Information System Risk Assessment (ISRA) must be completed using CMS-approved templates. Finally, others may either use a CMS template or a locally generated document such as the Security Impact Assessment (SIA).

**Key Point**- *Make sure that all CFACTS entries, including all security controls, are accurate and complete at all times. This will ensure that CFACTS-generated documents are accurate.*

### System Security Plan (SSP)[[13]](#footnote-14)

The SSP is the key document associated with the FISMA system security. It should provide an accurate, detailed description of the FISMA system itself, security requirements, and those controls that are actually in place to protect the system. This document is generated by CFACTS.

**Tip:** *It is a best practice to maintain older copies of SSPs as new versions are generated. Do not overwrite old SSPs; you never can tell when you might need an older version.*

### Information System Risk Assessment (ISRA)[[14]](#footnote-15)

The ISRA details the business and technical risks associated with a FISMA system. It shares high-level information from CFACTS, as well as specific risks noted, their criticality,

### Privacy Impact Assessment (PIA)[[15]](#footnote-16)

The Privacy Impact Assessment (PIA) is not simply a compliance step – it guides the full analysis of a system for privacy risks and controls. A PIA is a process for assessing whether appropriate privacy policies, procedures, business practices, and security controls are implemented to ensure compliance with federal privacy regulations. PIAs are published on HHS.gov and go through a three-year review process.

Before starting to fill out the PIA, obtain and review any available program and system documentation. This may include:

* Websites which explain the service or business process supported by the system;
* Information Collection Requests (ICRs) if the system collects information from the public and is subject to the Paperwork Reduction Act (PRA);
* Privacy Act Statements (PASs) and System of Records Notices (SORNs) if records in the system are subject to the Privacy Act;
* Agency IT Portfolio Summaries (formerly called Exhibit 53s) or any Major IT Investment Business Cases (formerly called Exhibit 300s);
* Enterprise Program Lifecycle Artifacts such as a System Security Plan (SSP); and
* Any handbooks or other guidance on how to use the system.

It may be possible to reuse language from these documents to respond to questions. However, make sure you review all copied text to verify that it is specific to the system being reviewed, is complete, and makes sense absent the rest of the document. Text copied from marketing materials and system planning documents may discuss functions that were never purchased or implemented. Text copied from a SORN or budget document may describe more than one system.

It is important to remember that the completed PIA/PTA Template may be published on HHS’s website where it will be available to the general public. For this reason, it should be written so that someone with no system knowledge, and limited IT knowledge, could understand its purpose and what information it collects, maintains, and shares.

Completing a PIA may require collaboration between several individuals including:

* The HEAR representative;
* The FISMA System Inventory representative;
* The Records or Information officer;
* The Senior Official for Privacy;
* The Office of General Council; and
* The Departmental Privacy Act Officer in the Office of the Assistant Secretary for Public Affairs (OS/ASPA).

### Third-Party Websites and Applications[[16]](#footnote-17)

The Office of Management and Budget Memorandum 10-23, Guidance for Agency Use of Third-Party Websites and Applications, requires that agencies assess their uses of third-party Websites and applications to ensure that the use protects privacy. The mechanism by which agencies perform this assessment is a privacy impact assessment (PIA). In accordance with HHS policy, operating divisions (OPDIVs) are responsible for completing and maintaining PIAs for all third-party Websites and applications in use. Upon completion of each assessment, agencies are required to make the PIAs publicly available. CMS implementation specifications are included in the ARS 3.1.

To view the CMS Third-Party Websites and Applications (TPWA) Privacy Impact Assessments for each individual OPDIV system, please refer to <https://www.hhs.gov/pia/index.html#Third-Party>

### Privacy Threshold Analysis

A Privacy Threshold Analysis (PTA) is a PIA for a system that does not contain PII or only contains HHS employee information. PTAs remain internal to HHS and do not have to go through the three-year review process. A PTA may be updated based on a major change to the system. It is also possible that change to a system could result in a PTA then meeting the threshold to be a PIA.

There are many resources available to help you complete PIAs and PTAs using the *PIA Template.*

* *PIA/PTA Writers’ Handbook* provides guidance about how to respond to the *PIA Template* questions.
* *HHS PIA Checklist* helps you complete a quality check of your PIA before submission.
* *Writers’ Handbook Quick Guide* allows you to quickly navigate the *PIA/PTA Writers’ Handbook.*
* The *HSDW Quick Reference* provides guidance on the review stages and how to create a new PIA.

The *Handbook*, *Checklist*, *Quick Guide,* and *HSDW Quick Reference* are available at: <https://community.max.gov/display/HHS/HHS+Privacy+Compliance+Working+Group>

## *Sidebar*: Contingency Planning[[17]](#footnote-18)

Contingency Planning provides instructions, disaster declaration criteria, and procedures to recover information systems and associated services after a disruption. It involves cooperation with your Business Owner, your data center or hosting facility, and senior CMS leadership.

As the ISSO, you will coordinate efforts with your Business Owner to determine the business criticality of key processes. This effort will result in a Business Impact Assessment (BIA) which, in turn, serves as the key requirement document for determining key recovery metrics including the Recovery Point Objective (RPO), Recovery Time Objective (RTO), Maximum Tolerable Downtime (MTD), and Work Recovery Time (WRT). The figure below shows the interrelationship between the metrics.

Recovery metrics can be thought of as follows:
RPO (recovery  point objective) is the time gap between business as usual and when a disaster occurs.
RTO (recovery time objective) is the time gap between when disaster occurs and when the system is recovered.  WRT (work recovery time) is the time from when the system is recovered until normal production is  resumed.  MTD (maximum tolerable downtime) is the sum of RTO and WRT.

Figure 3 Recovery Metrics

The goal is to ensure that there are plans in place to restore business functionality within the Maximum Tolerable Downtime. Note that this may involve restoring the system as originally constructed, moving to alternate processing facilities, or even moving to alternate processing methods.

### Contingency Plan (CP) Document[[18]](#footnote-19)

The CP Plan is a single document that contains:

* Key recovery metrics for your FISMA system;
* Pre-defined descriptions of conditions that constitute a need for action;
* Pre-defined actions based on the severity of an identified incident;
* Key staff, contact information, and specific duties for each person, and
* Item-level understanding of all of the hardware and software components of the FISMA system.

Items of Note:

* The CP must be attested to (signed) by the FISMA System Owner annually.
* All of the information necessary for the conduct of a contingency plan must be in the CP. There should be no references to offline personnel lists, contact information, system information, etc.
* All identified Key Personnel must have access to their own copy of the CP in a secure location that is accessible in the event that the FISMA system is unavailable.
* The CP, of all FISMA system documentation, must remain current.

### CP Plan Exercise[[19]](#footnote-20)

The CP must be tested at least once every 365 days. This is commonly referred to as the “Table Top”, but a table top test is only one (the easiest) way to exercise the CP. A test plan must be prepared and followed during the execution of the test. All staff who participate in an actual CP event must be available for the test.

**Key Point:** *Key staff members must be trained annually in their contingency responsibilities. It is best to perform this training immediately prior to the test. Training in this way refreshes individuals’ memories and ensures their availability for the test.*

**Tip:** *If your FISMA system is involved in an outage that causes you to exercise the CP Plan, you should consider documenting this event as an exercise of your CP Plan.*

### After Action

After the test is exercised, an after action report must be generated to describe the test and highlight specific deficiencies that must be corrected.

### CP Re-certification

After any corrections have been made, the updated CP Plan must be re-certified by the System Owner.

**Key Point:** *Make sure that all key staff members receive updated CP Plans that they have access to after hours; destroy (or return) older copies.*

## Assess Controls[[20]](#footnote-21)

The CMS Security Assessment and Authorization (A&A) Program protects the security and privacy posture of CMS systems throughout the system development lifecycle. As part of this program, all CMS systems are required to undergo assessments of risk and security/privacy control compliance prior to authorization. Assessments of risk and/or control compliance are conducted:

* When a new system is ready to be placed into an operational state;
* When a significant change has been made to an existing system;
* Annually, if a system follows a FISMA 1/3 assessment schedule;
* Ad hoc when requested or otherwise required; (*from Adaptive Capabilities Testing (ACT) Security and Risk Assessment Handbook Document Version: 1.1 December 20, 2019)*.

Currently there are two main types of assessments. Your component will dictate which type of assessment your system undergoes. In both cases:

* Plan and schedule your SCA/ACT as soon as possible. There may be some flexibility scheduling SCAs. With ACTs, you should try to schedule your ACT at least seven weeks before initiation.
* Make sure that all of your documentation is complete, and that it is housed in CFACTS appropriately.

### Security Controls Assessment. (SCA)

The Security Control Assessment, formerly known as a Security Test and Evaluation (ST&E), is a detailed evaluation of the controls protecting an information system. The security control assessment determines the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

### Adaptive Capabilities Testing (ACT)[[21]](#footnote-22)

ACT is a new assessment framework that CMS is actively developing to support various

transformative initiatives. The ACT framework is designed to be agile and extensible, and CMS

is actively evolving the process over time. ACT incorporates the concept of high-level *Security*

*Capabilities*, pioneered in other standards such as the Department of Homeland Security (DHS)

Continuous Diagnostics and Mitigation (CDM) program1 and National Institute of Standards and

Technology (NIST) Interagency Report (NISTIR) 80112. ACT also introduces the new concept

of *Risk Information Sources (RIS)*, which (as the name implies) are independent sources of

information about risks to a system or to the CMS enterprise that can be utilized to make risk-based decisions. ACT draws upon established and emerging standards such as NISTIR 8011, DHS CDM, and NIST Special Publication (SP) 800-53, for example. ACT is an important part of the process by which a system obtains its Authorization to Operate (ATO), helping CMS to:

* Validate that appropriate management, operational, and technical security and privacy controls have been implemented for the information system and working as intended;
* Identify and understand the risks that apply to the assessed system; and
* Identify and understand the risks that the assessed system and its environment pose to the CMS enterprise.

### Penetration Testing

Penetration testing is performed on information systems or individual system components to identify vulnerabilities that could be exploited by bad actors. Penetration testing is used to validate vulnerabilities or determine the degree of resistance that organizational information systems have to risk within a set of specified constraints (e.g., time, resources, and/or skills). This type of testing attempts to duplicate the actions of internal and external bad actors in carrying out hostile cyber-attacks against the organization and allows a more in-depth analysis. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls.

CMS has the ability to choose internal or external penetration testing teams; penetration testing is one of the services provided by the CCIC. For each penetration test, there must be an agreed upon Rules of Engagement (RoE) before the test can occur. The RoE ensures that a penetration test will be effective and safe for the environment and for those involved in the test itself. CMS utilizes its own RoE for penetration tests.

Penetration testing is performed on all High Value Assets (HVA) information systems within CMS at a frequency of every 365 days or when there has been a significant change to the system.

### Security Assessment Report (SAR) and CAAT File

In all assessments, a final Security Assessment Report (SAR) chronicles the results of the assessment. *The Risk Management Handbook (RMH) Chapter 4: Security Assessment and Authorization* states: “At the completion of a security controls assessment, the independent assessor completes a CMS Assessment and Audit Tracking (CAAT) spreadsheet. The CAAT spreadsheet is utilized for all CMS audits, assessments and penetration testing vulnerabilities. The completed CAAT spreadsheet is emailed to the CMS CISO mailbox at [CISO@cms.hhs.gov](mailto:CISO@cms.hhs.gov) for upload into the CFACTS tool. Once uploaded into CFACTS, the weaknesses are automatically generated for all items with a status of “other than satisfied”. The ISSO for the associated information system receives an automated email notification from the CFACTS tool identifying a new weakness. The ISSO has 30 days to create a POA&M within CFACTS.

## Plan of Action and Milestones (POA&M) Management

The POA&M is a remedial action plan (the process of accepting or resolving a risk) which helps the agency to identify and assess information system security and privacy weaknesses, set priorities, and monitor progress toward mitigating the weaknesses. A POA&M helps with tracking and mitigating the following [NIST SP 800-32]:

### Methods of risk mitigation

* Risk Avoidance: Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. Risk avoidance is usually the most expensive of all risk mitigation options.
* Risk Transference: Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on their core competencies.
* Risk Acceptance: Risk acceptance does not reduce any effects however it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn’t want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

Note: Risk acceptance has relatively high visibility within CMS. The process, although relatively straightforward, is commonly misunderstood.

Although all decisions regarding security are or should be risk-based, you most likely will hear the term **Risk Based Decision (RBD)** used exclusively to mean risk acceptance.

* + RBD is not intended to substitute for other, preferred forms of risk mitigation. It should be used only when the residual risk cannot be further mitigated without excessive expense and with the express permission of the Authorizing Official, the CMS Chief Information Officer (CIO).
  + Note that, when approved, the RBD must be reevaluated every year, or as otherwise indicated.
* Risk Limitation: Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company’s exposure by taking some action. It is a strategy employing a bit of risk acceptance along with a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

An organization decides the level of risk is acceptable to work with. “Risk Tolerance” is defined as the level of risk an entity is willing to assume in order to achieve a potential desired result.

A POA&M is required for every system where an IT security or privacy weakness has been found. The findings stem from internal or external audits, reviews, and Continuous Diagnostic and Mitigation (CDM). Each finding identifies a weakness that must be resolved according to a POA&M.

POA&M Corrective Action Plan (CAP) describes the measures that have been implemented or planned: (i) to correct any deficiencies noted during the assessment of the security and privacy controls; and (ii) to reduce or eliminate known vulnerabilities in the information system. It identifies: (i) the tasks needing to be accomplished; (ii) the resources required to accomplish the elements of the plan; (iii) any milestones with scheduled completion dates.

A POA&M must have at least one milestone. Once a milestone has been accepted and closed, the record must be retained for one year. Milestones should be S.M.A.R.T:

* Specific – target a specific area for improvement.
* Measurable – quantify or at least suggest an indicator of progress.
* Assignable – specify who will do it.
* Realistic – state what results can realistically be achieved, given available resources.
* Time-related – specify when the result(s) can be achieved.

A POA&M can be used for the following reasons:

* Assist management in identifying and tracking the progress of corrective actions
* Assist agencies in closing their security and privacy performance gaps
* Assist the Office of Inspector General (OIG) in evaluating agency security and privacy performance
* Assist OMB with its oversight responsibilities and the budget formalization process
* Assist with Congressional oversight by providing pre-decisional budget information

### Reports

Reporting is a critical component of POA&M management, and CMS reports its remediation efforts on a monthly basis. The information in the POA&M must be maintained continuously to communicate overall progress.

OMB typically requires reporting on a quarterly or annual basis. Quarterly reports are usually focused on a specific area of interest. The reports are prepared by the CISO Office and provide the required information to DHHS on a quarterly basis for verification and analysis. DHHS compiles the information and sends a consolidated report to OMB.

### POA&M Closing Requirements

POAMs must be addressed/remediated in a timeframe depending on the severity of the reported vulnerability. They are:

* Critical vulnerabilities: 30 days
* High vulnerabilities: 60 days
* Medium vulnerabilities: 90
* Low vulnerabilities: 180

**Note:** *These timeframes may change. Consult the latest policy for POA&M requirements.*

## Authorize the System[[22]](#footnote-23)

“Security authorizations are official management decisions that are conveyed through authorization decision documents by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. The CIO serves as the authorizing official for CMS. The CIO is responsible

for making an overall determination of risk and authorizing CMS information systems for operation, if it is determined that the associated risks are acceptable. An ATO memo is signed by the CIO giving the System Owner/BO formal authority to operate a CMS information system.”

There are three NIST document requirements for an ATO “package” and six more that are specific to CMS. The documents include:

* System Security Plan (SSP)
* Security Assessment (Final) Report (SAR)
* Plans of Action and Milestones (POA&M)
* Contingency Plan (CP)
* CP Test Plan
* CP Test After Action Report
* Information System Risk Assessment (ISRA)
* Privacy Impact Assessment (PIA)
* Interconnection Security Agreement (ISA) – *as applicable*

Risk Management Handbook (RMH) Chapter 4: Security Assessment and Authorization, Version 1.0, Section 6.4 provides detailed instructions.

## Continuous Monitoring

“Continuous monitoring” has been a rapidly-evolving program at CMS. As an ISSO you will work closely with the ISPG CCIC to ensure that your system is appropriately monitored. CCIC ensures oversight of information security and privacy, including Security Information Event Management, for each FISMA system operating by or on behalf of CMS. The CCIC delivers various agency-wide security services. These services include Continuous Diagnostic and Mitigation (CDM) as well as security engineering, incident management, forensics and malware analysis, information sharing, cyber threat intelligence, penetration testing, and software assurance.

Risk Management Handbook (RMH) Chapter 4: Security Assessment and Authorization, Version 1.0, Section 6.5 provides detailed information.

## *Sidebar*: Managing Security Incidents[[23]](#footnote-24)

*Known or suspected security or privacy incidents involving CMS information or information systems must be reported immediately to the CMS IT Service Desk by calling 410-786-2580 or 1-800-562-1963, or via e-mail to* [*CMS\_IT\_Service\_Desk@cms.hhs.gov*](mailto:CMS_IT_Service_Desk@cms.hhs.gov)*. Additionally, the system’s ISSO should also be contacted as soon as possible and apprised of the situation.*

## ISSO Recurring Tasks

This section provides a list of tasks an ISSO should perform periodically. The period of performance listed for each task provides a general guideline which may vary depending on the Component guidance or system circumstances.

### Ongoing Activities

The following activities need to be performed on a periodic basis (at least annually). They require regular effort throughout the year:

* Security control assessment SCA/ACT/Pen Test;
* Review and update the Security Authorization Process documentation to include SSP, ISRA, CP, PIA, and CP test (most often a Table Top Test). Documentation should be updated as changes occur, but each requires an annual review and update;
* Incident response report (as required);
* ATO update (as required).
* Respond to CCIC monitoring alerts as required.

#### Weekly Activities

* + Review audit logs;
  + Routinely evaluate risk posture based upon change requests;
  + Ensure that data is backed up;
  + Check POA&M status.

#### ISSO Monthly Activities

* + Review/deactivate unused accounts.

#### ISSO Quarterly Activities

* + Ensure that all data in CFACTS is current and accurate one week before the end of the quarter. CMS submits a quarterly FISMA report to OMB based on this data.

### ISSO Annual Activities

The following activities need to be completed annually, and require an effort over several months to complete:

* Ensure that all system users and people with security responsibilities (e.g., ISSOs) receive their required annual awareness training;
* Conduct a Contingency Plan Test (most often a Table Top Test);
* Review the Privacy Impact Assessment;
* Ensure that vulnerability assessments are completed at least annually;
* Vulnerability scans should be conducted at least annually, or when significant changes are made to the system, or when directed;
* Review and validate user access rights.

### As Required Activities

* Update the SSP whenever there are system or personnel changes, but at least annually;
* Review change requests that have been forwarded and/or recommended, and be prepared to assist with Security Impact Assessment (SIA) to help the Business Owner understand the potential risk associated with a potential change;
* Participate in the development phases of the system life cycle;
* Ensure that all system users understand and sign the Rules of Behavior (ROB) before being granted access;
* Report compliance on secure protocol use in websites periodically as defined within the ARS.

# Chapter 5: ISSO Tools

## ISSO Welcome Packet

If you are a new ISSO the Welcome Packet is the place to start. This document serves as a welcome to the ISSO Community, and contains information that brand-new ISSOs will find helpful. The easiest way to get this document is to email [ISSO@cms.hhs.gov](mailto:ISSO@cms.hhs.gov) to get a copy.

## ISSO Mentoring

The ISSO Mentorship Program provides an ongoing educational program that further enhances the knowledge, skills and abilities of a CMS ISSO in support of the CMS information systems security and privacy program. Continuing professional education is important to maintain and enhance the ISSO’s knowledge and level of competency. Security technology is fast growing and quickly changing. Keeping up to date and expanding the ISSO’s knowledge base increases the individual’s value to the agency.

This program is not a substitute or a replacement for the CMS Mentoring Program. Rather, it is structured to give the ISSO mentee access to the experience and expertise of senior security professionals for career management, self-development, and system security support. The relationship provides an opportunity for the ISSO to further enhance their knowledge, skills and abilities in support of CMS’ information systems security.

The goal of this program is to improve the useful sharing of security best practices and organizational insights on what really works among Cybersecurity professionals. This program would support the ISSOs as they continue to develop the knowledge and skills needed to continually improve the security posture of CMS.

* Strengthen the CMS cybersecurity community by building stronger personal ties among ISSOs.
* Enhance the careers and professional opportunities available to participants.
* Encourage an open exchange of ideas and questions in a nonthreatening environment.

Mentoring can benefit everyone. Mentor relationships, whether formal or informal, are a key to enabling success in both personal and professional lives. The mentoring program can lead to new ISSOs acquiring knowledge and expertise more efficiently. The program can also offer other benefits, such as increasing employee retention and work productivity. The mentor relationship helps mentees work out what they want to achieve and how to get there, while benefiting the mentor in the capacity as a role model. Mentors are much more than coaches. They help the whole individual develop by providing advice and resources, supporting career goals, and celebrating achievements.

The mentor is a senior security professional who has had his or her skills and knowledge validated via an industry recognized certification program and is an active holder of such certification as the CISSP, CISA, or CISM. The mentor should also have at least five years’ experience in information systems security and five years’ experience in the Federal government. The mentor would provide the ISSO with a wealth of knowledge and experience, thereby improving the individual’s knowledge, skills and abilities. The level of involvement and interaction would be up to each ISSO.

## The “ISSO Toolbox”

To support the ISSO role, it is important and beneficial to know and utilize the advantages of all available resources. The following sections describe references, tools and other resources ISSOs should include in their toolkits.

### CISO Mailbox

Do you have a question or concern related to CMS information security or privacy? If you are an ISSO, your first connection should be to your CRA. If they are not available, send an email to the CISO Team at CISO@cms.hhs.gov regarding information security, or an email to [Privacy@cms.hhs.gov](mailto:Privacy@cms.hhs.gov) for questions regarding privacy.

### CMS Information Security and Privacy Website

The Information Security and Privacy Library is intended to serve as a one-stop resource for all of your information security needs. The library contains a comprehensive listing of policy guidance, standards, regulations, laws, and other documentation related to the CMS Information Security and Privacy Program.

### CMS ISSO Framework

The CMS ISSO Framework was developed to primarily support the ISSO role by identifying and centralizing the processes, elements, and requirements for maintaining the security and privacy posture of Information Technology (IT) systems at CMS.

The Framework aligns key responsibilities to the Framework for Improving Critical Infrastructure Cybersecurity, developed by the National Institute of Standards and Technology (NIST) which are comprised of the functions of: Identify, Protect, Detect, Respond, and Recover. The ISSO Framework also includes a section which centrally identifies key authoritative references including those from NIST, HHS, CMS, and the Office of Management and Budget (OMB).

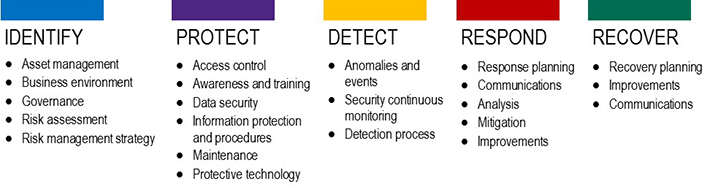


Figure 4 NIST Cybersecurity Framework

The Framework enables the ISSO to apply the principles and best practices of risk management to improving the security and resilience of their systems. It establishes the common taxonomy and lexicon used to describe all ISSO cybersecurity work. The Framework is intended to support both Federal and contractor ISSOs across CMS so that individuals and organizations may effectively conduct cybersecurity work.

The ISSO oversees the information assurance program of an information system in or outside the network environment and may include procurement duties. More specifically, the ISSO oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that information technology systems meet the organization’s information assurance and security requirements. The Framework supports the appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

### ISSO SharePoint Site

The CMS ISSO SharePoint Site holds information that is useful to all ISSOs. It includes past ISSO Forum minutes, ISSO Journals, notes from past meetings, and other items of interest. Note that access to internal cms.local is required to reach this information.

### ISSO Forum

The CMS ISSO Forum held monthly is an opportunity for the CMS cybersecurity community to exchange information; to share knowledge and to assess and solve information security problems as a community. It provides opportunities to review CMS’ security related strengths, weaknesses, threats and opportunities and reinforces CMS’ strategies, goals and action programs.

#### Purpose

The purpose of the ISSO Forum is to:

* Provide a conduit for two-way communication with the CMS security community
* Provide a venue for ISPG to disseminate critical information
* Distribute critical metrics and information regarding ISPG priorities
* Provide up-to-date ISPG guidance regarding security and privacy policies and updated procedures
* Address current topics and provide guidance to overcome the wide-ranging security challenges that impact CMS business
* Address common questions and solutions from the ISSO community

Format:

* Meeting minutes and questions will be captured and distributed to all attendees
* Request for agenda topics will be distributed 7-14 days prior to the meeting
* Topics should include both what ISPG needs to push out to the ISSO community and what the ISSO community is asking questions about or needing support
* The meeting’s message should align with the ISPG Strategic Plan

#### Meeting Structure

*Conference room and moderated WebEx meeting*

* Participant attendance will be documented
* Participant’s phones will be muted
* 508 compliant

*Agenda Format*

* Final agenda will be sent out to ISSO community 5 business days prior to the meeting.
* All meetings will be recorded using the WebEx recording function
* Attendance and meeting minutes will be taken and distributed to attendees five business days after the meeting and also published to a SharePoint site.
* Questions and answers will be tracked in a separate QA sheet that will be attached to the distributed minutes

*Meeting Layout*

* Agenda
* Topic 1- 10-15 minutes
  + Questions – 5 minutes
  + Question format – open microphone and chat box
* Topic 2 – 10-15 minutes
  + Questions – 5 minutes
  + Question format – open microphone and chat box
* Standing ISPG topic – 10-15 minutes
  + Questions – 5 minutes
  + Question format – open microphone and chat box

#### Topics & Contributors

* Potential Topic Contributors:
  + ISSOs
  + CISO’s Office – Division directors, Cyber Risk Advisors, Security SMEs
  + Training team
  + Data Guardian
  + TRB
* Topic Examples
  + Delayed POA&Ms statistics with step by step procedures in CFACTS for updating milestones and closing POA&Ms
  + PIA statistics with processes for completing PIAs in CFACTS and submitting them for ISPG review
  + ISSO Framework
  + Security Impact Analysis
  + Data Guardian / ISSO Relationship
* Potential Presenters:
  + ISSOs
  + Anyone from the CISO’s office including contractor support
  + Data Guardian
  + Technical Review Board members

### ISSO Journal

The ISSO Journal is published on a bimonthly schedule. The Journal editors seek to solicit and provide information that is relevant to CMS ISSOs and contractor security support individuals. Each issue has one or more feature stories that include information relevant to CMS security professionals, along with regular columns and features by CMS ISPG staff. The Journal can be found on the CMS ISSO SharePoint site and also on the CFACTS home page.

# Chapter 6: Important Reference Information

Chapter four introduced the ARS in detail since it is key to understanding the specific tasks presented. The following references are also necessary to effectively perform as an ISSO.

## HHS Information Security and Privacy Policy (HHS IS2P)[[24]](#footnote-25)

The IS2P comprises HHS policies and procedures that ensure the collection, use, sharing, storage, and security of information that is both terrorism-related information and “protected information (PI)”. Where possible, this document identifies existing HHS policies and procedures that meet the privacy requirements. Where necessary, however, this document also creates policies specific to the activities and resources that HHS requires. The IS2P is one of the base documents from which CMS requirements flow.

## CMS Information Security and Privacy Policy (CMS IS2P2)[[25]](#footnote-26)

The IS2P2 defines the framework under which CMS protects and controls access to CMS information and information systems. It provides direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems; systems maintained on behalf of CMS; and other collections of information to assure the confidentiality, integrity, and availability of CMS information and systems. Along with the Acceptable Risk Safeguards highlighted earlier, the IS2P2 constitute one of the core reference sources for cybersecurity policies and practices at CMS.

## Information Security and Privacy Library

The best thing that you can do as an ISSO is to read the directions first. Guidance for every task that you must accomplish can be found in the Information Security and Privacy Library. It is a compilation of CMS standards, requirements, directives, practices, and procedures for protecting CMS information and information systems. Access the Library at <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>.

Note: In addition to the CMS-wide instructions, make sure that you are also thoroughly familiar with any component guidance applicable to your system(s).

## CMS Risk Management Handbooks

Risk Management Handbooks (RMH)s are core documents found in the Information Security and Privacy Library.

RMHs are designed to help ISSOs understand and address the many CMS security and privacy requirements developed to protect their system(s). The RMHs are generally aligned to provide specific guidance and recommendations for specific ARS Control Families. For example, RMH Chapter Six, Contingency Planning, addresses the ARS controls in the CP Family. As you work through your ARS controls, you should have the appropriate RMH handy. Appendix E, RMH Quick Guide, provides a quick reference for current RMHs, along with the key topics contained within each Guide.

Tip: *Make sure that you check the Security and Privacy frequently, as documents are updated and added relatively frequently.*

## NIST Special Publications

NIST Special Publications in the 800 series are of general interest to the computer security community. There are more than 100 NIST Special Publications relating to everything from the Security Authorization Process to specific guides for implementing various technology solutions (e.g., Bluetooth, Secure Web Services, etc.). They serve as the basis for CMS security policies and procedures. However, ISSOs need to be aware CMS has tailored NIST guidance for application within the Agency. While NIST should be used to provide general guidance, ISSOs should rely on Agency specific guidance.

While most NIST Special Publications are useful as general references, NIST SP 800-53: Recommended Security Controls for Federal Information Systems and NIST SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems are two of the most important for ISSOs. They contain detailed explanations of information security controls and the test cases used to assess them. All ISSOs should be thoroughly familiar with both of these documents. NIST SPs are available at <http://csrc.nist.gov/publications/PubsSPs.html>.

## CMS Information Security Contract Clause/Provision

CMS has modified its contracts and solicitations for the incorporation of a CMS Information Security clause/provision to safeguard information and information systems that support the operations and assets of the agency, including those provided or managed by contractors (including subcontractors) on behalf of the agency. Click here: <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

## Security in the System Development Lifecycle (SDLC)

In Chapter Four, the TLC and XLC were briefly discussed. The TLC has replaced the XLC as the official CMS IT Governance and System Development Life Cycle framework.  This single governance framework accommodates alternate IT development methodologies, while still meeting all applicable legislative and policy requirements.

If your current projects or contracts specify the use of XLC-related tools, templates, or reviews, you may continue using them.  You may also use fewer or alternative tools and templates, as long as you meet the minimum requirements outlined within the TLC.

For new systems, enter the TLC by submitting an [IT Intake Form](https://share.cms.gov/Office/OIT/CIOCorner/Lists/Intake/NewForm.aspx) when you:

* Initiate a new IT project
* Conduct an acquisition to support a new IT project
* Request new/increased funding to support an IT project
* Plan significant changes to an existing IT project

After submitting your form, the CMS IT Governance Team will help you meet TLC requirements.

If you or your contractors want more information, please visit [the TLC page](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/TLC) on CMS.gov. CMS employees may also contact the [IT Governance Team](mailto:IT_Governance@cms.hhs.gov).

## Spotlight

The CMS “Spotlight” portal keeps you up-to-date with the latest changes to CMS and related Federal policies and also highlights many of the foundational components of the CMS information security and privacy program. Here you will find many of the most current, common standards, procedures, and policy documents applicable to CMS.

## Enterprise User Administration

A CMS User ID serves as your “virtual security badge,” for CMS Networks, granting you access to information and resources that you are authorized to see and preventing access to information and resources that you are not authorized to see. Management of most CMS User ID’s is accomplished through the Enterprise User Administration (EUA) system. Additional information regarding the system can be found under the “CMS System User Information” heading.

## OMB Memoranda

Every year OMB publishes a Memo with reporting instructions and guidance for FISMA (e.g., M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management). Memos are available at: <http://www.whitehouse.gov/omb/memoranda_default/>

## OMB Circulars

There are a number of OMB Circulars that provide general guidance on information security. Three of the most relevant are:

* A-130 - Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources
* A-123 - Management's Responsibility for Internal Control
* A-127 - Financial Management Systems

OMB A-130 applies to all IT systems while A-123 and A-127 apply primarily to financial systems. ISSOs should be aware of these foundation documents and have a general understanding of their content. They can be found at: <http://www.whitehouse.gov/omb/circulars_default/>

# Chapter 7: Training

## Introduction

People come to the ISSO role from many backgrounds, with differing experiences, so each may start at a different place. This section and the appendices following give new ISSOs a broad idea of where to go, what to do, and in what sequence training should be addressed. A nationally-developed framework is discussed, which frames training and knowledge requirements based on role.

## Getting Started

Broadly, ISSOs need to have both doctrinal cybersecurity knowledge and specific knowledge of how things operate at CMS to be successful.

 **Cybersecurity knowledge.** Every professional needs to understand the theory and technology that underpins their vocation. Cybersecurity is a complex field that encompasses elements of technology, privacy, law, and an understanding of business issues. If you are new to cybersecurity you have probably already worked in many of these areas; you will probably need to branch out.

 **CMS-specific application knowledge.** Even cybersecurity experts from outside CMS need to know and understand CMS’ interpretation of cybersecurity practices and, more especially, the Federal government’s rules.

## The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Overview

The NICE Framework, NIST Special Publication 800-181, establishes taxonomy and common lexicon that is to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

The NICE Framework is comprised of the following components:

* Categories (7) – A high-level grouping of common cybersecurity functions;
* Specialty Areas (33) – Distinct areas of cybersecurity work;
* Work Roles (52) – The most detailed groupings cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks in a work role;
  + Knowledge, Skills, and Abilities (KSAs) – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.
  + Tasks – Specific defined pieces of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role.

The NICE Framework serves several key audiences within the cybersecurity community including:

* **Employers**, to help assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions;
* Current and future cybersecurity **workers**, to help explore Tasks and Work Roles and assist with understanding the KSAs that are being valued by employers for in-demand cybersecurity jobs and positions. The NICE Framework also enables staffing specialists and guidance counselors to use the NICE Framework as a resource to support these employees or job seekers;
* **Training and certification providers** seeking to help current and future members of the cybersecurity workforce gain and demonstrate the KSAs;
* **Education providers** who use the NICE Framework as a reference to develop curriculum, courses, seminars, and research that cover the KSAs and Tasks described; and
* **Technology providers** who can identify cybersecurity Work Roles and specific Tasks and KSAs associated with the services and hardware/software products they supply.



Figure 5 NICE Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: The Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

## Sources

There are many external sources, professional organizations and training organizations offering information and training.

* You should first take a look at the training provided by CMS. The CMS CBT site at **www.cms.gov/cbt** is an entry point for information and training that will help. You should also review the **CMS Cybersecurity and Privacy Catalog** for upcoming courses, Webinars, and other information.
* The HHS Learning Management System (LMS) offers Skillsoft courses that you can take, for free, to further both your cybersecurity core knowledge and that can prepare you for certification.
* The Federal Virtual Training Environment (FedVTE) provides another source of free training, similar to LMS.

## Recommended Training Sources, by Experience

The following three tables present some training opportunities, based on ISSO experience level.

### Recommended ISSO Training Courses – Basic

The courses listed below will provide both an introduction to cybersecurity in general and guidance on how these concepts are implemented at CMS. You should place your emphasis on the courses listed in bold. You should consider some or all of the rest of the courses as your time permits. **If all possible, you should try to complete the bolded courses within your first two months as an ISSO**. There is no cost to take these courses.

|  |  |
| --- | --- |
| **Course** | **Source** |
| **ISSO Fundamentals** | CBT |
| **Working with CFACTS** | Classroom/Remote |
| **All About the CMS Acceptable Risk Safeguards (ARS) 3.1** | CMS |
| Executive’s Guide to Security: Protecting Your Information | LMS |
| Executive’s Guide to Security: Understanding Security Threats | LMS |
| Compliance Expert: Privacy and Information Security-The Basics | LMS |
| Compliance Short: Privacy and Information Security | LMS |
| Compliance Short: Privacy and Information Security 2 | LMS |
| Cybersecurity 101-Session and Risk Management | LMS |
| **Privacy and Information Security** | LMS |

### Recommended ISSO Training Courses – Intermediate

The courses listed below will build on your initial knowledge. As before, you should place your emphasis on the courses listed in bold, or on topics that have immediate importance to you. There is no cost to take these courses. You should place your emphasis on the courses listed in bold.

|  |  |
| --- | --- |
| **Course** | **Source** |
| Navigating New Cybersecurity and Privacy Policies and Procedures | CMS |
| How Hackers Hack and How to Protect Yourself | CMS |
| Your Role in Privacy at CMS | CMS |
| **Incident Response at CMS** | CMS |
| CMS Privacy Incident Response: Quick Guide for Business Owners | CMS |
| Cybersecurity Race | CMS |
| **Cyber Risk Management for Managers** | FedVTE |
| **Cyber Security Overview for Managers** | FedVTE |
| Foundations of Incident Management | FedVTE |
| Compliance Expert: IT Security-Phishing | LMS |
| Cybersecurity 101-Auditing and Incident Response | LMS |
| Information Security Incident Management 1 | LMS |
| Information Security Incident Management 2 | LMS |
| **Selecting Software Security Controls** | LMS |
| Troubleshooting Common Security Issues | LMS |

### Recommended ISSO Training Courses – Advanced

These advanced courses will help you gain a deeper understanding of the cybersecurity issues that you have been working with. They may also be appropriate to take earlier if you entered the ISSO role with a good basic understanding of both CMS operations and cybersecurity in general. There is no cost to take these courses. You should place your emphasis on the courses listed in bold.

|  |  |
| --- | --- |
| **Course** | **Source** |
| Emerging Cyber Security Threats | FedVTE |
| Securing Infrastructure Devices | FedVTE |
| Securing the Network Perimeter | FedVTE |
| **Cloud Computing Fundamentals; Cloud Security** | LMS |
| **Cloud Data Security** | LMS |
| **Cloud Security Fundamentals: Legal and Compliance** | LMS |
| Cloud System Security: Platform and Infrastructure | LMS |
| Security Fundamentals: Authentication | LMS |
| **Security Fundamentals: Authentication, Passwords and Audit Policies** | LMS |
| Security Fundamentals: Client and Email Security | LMS |
| Security Fundamentals: Core Security | LMS |
| Security Fundamentals: Encryption and Malware | LMS |
| Security Fundamentals: Firewalls | LMS |
| Security Fundamentals: Internet and Wireless Security | LMS |
| Security Fundamentals: Network Isolation | LMS |
| Security Fundamentals: Permissions | LMS |
| Security Fundamentals: Protocol Security | LMS |
| Security Fundamentals: Server Protection | LMS |

As an ISSO, you have many options for training in the CMS and HHS environment. Upcoming appendices give further information on certification programs, and discuss how you can plan for them during your career as an ISSO. A proposed ISSO Certification Levels Recommendation table is presented in Appendix B. You can look at this table and insert your accomplishments and experience to get a rough idea of where you stand in the ISSO experience continuum.

# Appendix A: Cybersecurity Certifications

The dynamic nature of cybersecurity requires ISSOs to proactively learn about changes in threats and vulnerabilities to our agency’s information systems. Cybersecurity training and certifications help equip ISSOs to understand these threats and maintain the security posture of your systems. Training courses range in scope from general security awareness and online user safety, to practical instruction and highly technical advanced certifications. Industry-recognized Certifications validate an ISSOs specific skill or experience in a particular subject area.

***Popular Cybersecurity Certifications***

* CompTIA A+, Network+ and Security+
* EC Council Certified Ethical Hacker (CEH)
* ISC2 Certified Information Systems Security Professional (CISSP) and Certified Information System Manager (CISM)

This section introduces some of the most prominent certifications for consideration.

The HHS Learning Management System offers over 190 security and privacy related classes including preparation courses for CISM, CISSP, Cybersecurity Analyst+ and Security+.

The Federal Government provides IT Professionals numerous opportunities to develop their knowledge, skills, and abilities and attain professional certifications for their work. For example, the U.S. Department of Defense has specified several security-related certification programs for their employees with their Information Assurance Workforce Improvement Program.

The following information pertains to some popular IT certifications that many Federal agencies recommend and oftentimes require their IT workers to hold.

## Federal IT Security Professional Certification (FITSP)

While all other certification programs are often generalist in nature, the Federal IT Security Professional Certification takes into consideration what your skills are and what you know, while also certifying that these are in tune with Federal best practices and standards. It is open to IT professionals already working in government.

The FITSP Certification has four different roles that a candidate can choose from:

* Manager - For those who oversee IT security in their organizations, such as Information Assurance Managers, Chief Information Security Officers, and Information Security Managers.
* Designer - For system developers and designers and other engineers who are responsible for developing and designing an IT system.
* Operator - For database administrators, ISSOs and other personnel who manage, maintain and operate information systems.
* Auditor - For public accountants, inspectors and other professionals who audit and review an information system.

The FITSP Certification Exam is a 150-question, computer-based exam that costs $295[[26]](#footnote-27). A passing score is cut-off at 75%. Candidates who fail in an FITSP exam can take a similar one at a 50% discount in the future.

## CompTIA A+ Certification

The Computing Technology Industry Association's A+ Certification is for those who are in federal IT support departments. It validates that an individual has all the necessary skills and knowledge for the job of installing, maintaining, securing and troubleshooting IT systems.

To be certified, you would need to pass two exams:

* CompTIA A+ Essentials - A 90-question examination requiring a score of 675 out of 900 to pass. You need to have at least nine to 12 months hands-on experience and this would test you on computer technology, security, networking and even professionalism and communication skills.
* CompTIA A+ Practical Applications - A 90-question examination requiring a score of 700 out of 900 to pass. This will test you on the more practical applications of the skills pinpointed for the CompTIA A+ Essentials exam.

## CompTIA Network+

The Computing Technology Industry Association's Network+ Certification is for those who are in federal IT support departments. It validates that an individual has all the necessary skills and knowledge for the job of installing, maintaining, securing and troubleshooting IT systems.

To be certified, you would need to pass one exam:

* CompTIA Network Essentials - A 90-question examination requiring a score of 720 out of 900 to pass. You need to have at least 500 hours of hands-on experience and this would test you on computer technology, security, networking and even professionalism and communication skills.

## CompTIA Security+

CompTIA Security+ is a certification exam for IT security professionals. It gauges your competency in network security, access control, identity management, compliance, operational security, detecting and handling vulnerabilities and threats, host, data, application security, and cryptography.

Security architects, information assurance technicians, security administrators, systems administrators, network administrators and systems consultants will be tested to see if they have sufficient knowledge in the tools, procedures and concepts of security, anticipating risks and protecting the system.

This is a 90-question exam requiring a score of 750 out of 900. Certification requires at least two years of experience in technical networking with a focus on security-related functions and a CompTIA Network+ certification.

## (ISC)2 System Security Certified Practitioner (SSCP)

The International Information Systems Security Certification Consortium is also home to the CISSP, the best-known senior-level security certification. Those interested in pursuing the SSCP need to possess at least one year of experience in one or more of the seven SSCP Common Body of Knowledge domains. Candidates must also pass an exam to obtain the credential. Those who do not yet meet the experience requirement may choose to first obtain the Associate of (ISC)2 certification, which is available to any candidate who passes the CAP, CCFP, CISSP, CSSLP, HCISPP or SSCP exam.

## SANS GIAC Information Security Fundamentals Certification (GISF)

The SANS Institute is a long-standing and well-recognized organization in the security industry. Likewise, its GIAC certifications continue to accrue visibility and acceptance. The GISF opens the door to other credentials in the respected SANS GIAC program. Since the GISF is an entry-level credential, there are no prerequisites; candidates need only pass a single exam to obtain the credential.

## Microsoft Certification Programs

There are Microsoft Certifications for all skill levels covering most technologies produced by Microsoft. These are classified into six levels:

* Microsoft Certified Architect – Advanced certification for architects.
* Microsoft Certified Master – Certifies experienced IT professionals and their ability to meet even the very complex requirements of a business.
* Microsoft Certified IT Professional – Certifies that an IT professional knows how to deploy, support and optimize different IT infrastructures.
* Microsoft Certified Professional Developer – Certifies that IT professionals have the requisite skills to design, develop and deploy applications that are required in their own jobs.
* Microsoft Certified Technology Specialist – Shows in-depth expertise and knowledge in various technologies and platforms.
* Microsoft Technology Associate – Helps students and undergraduates explore job options in IT and technology. This also prepares personnel for other Microsoft Certified Technology Specialist exams and other advanced studies.

You need a Microsoft Certified Professional Developers certification level for your specific job function. For example, get a Microsoft Certified Systems Engineers certification if you work as a system analyst, systems engineer, technical consultant, support engineer, or a network analyst. The Microsoft Systems Administrator program can show that you can implement systems and troubleshoot them within a Windows Server environment.

Examinations for the Microsoft Certified Professionals certification vary in cost and have around 40 to 90 multiple-choice questions.

## ITILTM Certification

The Information Technology Infrastructure Library Certification (ITIL™) signifies that the individual has sufficient knowledge of the best practices involved in IT service management.

There are several levels of ITIL™ Certification.

### Foundation

This is the most basic level of certification, which proves that the individual has learned all the terminology, basic concepts and structure espoused by ITIL™. This involves at least 18 hours of instruction and a 40-question multiple-choice exam. Passing score is 65%.

### Intermediate

This actually has two tracks: Service Lifecycle and Service Capability. Service Lifecycle is focused on the different stages of strategy, design, transition, operation and improvement. It needs at least 21 hours of instruction, and a 70% passing score on an 8-question multiple-choice exam. The Service Capability track, on the other hand, involves four different modules. This requires at least 30 hours of instruction and at least a score of 70% on an 8-question multiple-choice exam. You also need to have an ITIL™ Foundation certification or its equivalent.

### Managing across the Lifecycle

This level basically completes the two Intermediate tracks by providing the individual with the skills to implement either track. It focuses on the management and implementation of Lifecycle practices. This requires at least 30 hours of instruction and a score of at least 70% on several multiple-choice questions.

### Expert

To be certified as an ITIL™ Expert, you would need at least 22 credits from the first three levels of ITIL™ certification.

## Advanced Certifications

Premium or senior-level security certifications require three or more years of relevant, on-the-job experience. Many also require submitting papers or research results in addition to passing exams, as well as taking specific classes.

### CompTIA Advanced Security Practitioner (CASP)

The CASP is intended as a follow-on to Security+ and is intended to recognize IT professionals with three or more years of direct, day-to-day information security experience, with skills and knowledge to match. The CASP requires continuing education for maintenance or a re-take of the exam every three years. It costs around $390, which is less than the CISSP, but it is ranked the same for a variety of Department of Defense-related IT positions, which will no doubt contribute to its future popularity. CompTIA announced an update to the CASP certification exam in February 2015 that includes new questions about contemporary threats as well as troubleshooting processes related to data, endpoint and network security.

### Certified Information Systems Security Professional (CISSP)

The Certified Information Systems Security Professional (CISSP) covers a wide range of information technology and security topics focused on the following:

* Access Control
* Cryptography
* Network Security
* Operations Security
* Risk Management& Security Governance
* Security Architecture & Design
* Software Development Security
* Disaster Recovery Planning & Business Continuity
* Legal, Compliance, Regulations, & Investigations
* Physical Security

The CISSP is provided by (ISC)2. To be certified you would need:

* At least five years of experience in information technology security focused on the ten areas specified above or an equivalent educational degree or certification from similar organizations.
* To accept the organization's Code of Ethics and answer queries about one's background.
* To get a score of 700 points out of the 1000 possible score in a 250-question multiple-choice examination that can take 6 hours to complete.
* An endorsement from another CISSP member.

If you do not have the necessary experience or educational background you could still get certified as an (ISC)2 Associate.

### SANS GIAC Security Certifications

SANS Global Information Assurance Certification offers numerous topical specializations that extend the GISF and the GIAC Security Essentials Certification (GSEC), including firewalls, incident handling, intrusion analysis, Windows and UNIX administration, information security officer and systems and network auditor certifications. This is a topical, timely and highly technical program based on outstanding training online or at SANS conferences. For those willing to acquire four of these individual credentials (two of them "gold") and sit for a lengthy exam in two parts, moving on to the GIAC Security Engineer (GSE) certification probably makes sense.

### Cisco Certified Network Associate (CCNA)

Although it is vendor-specific, the Cisco Certified Network Associates is quite popular among IT professionals working in the federal government because it also prepares them to work with other protocols. This certification signifies that the individual has all the necessary skills and knowledge to administer different Cisco devices on their networks. It has different tracks, including:

* Security
* Wireless
* Voice
* Routing and Switching
* Service Provider Operations

These exams, costing approximately $100, typically have about 78 questions that take 2 hours to answer. Passing scores differ, but generally you should get more than 80% of the questions.

## In Summary

If you are considering becoming a CMS ISSO or have recently been appointed and you don’t have much experience with security; work with a seasoned ISSO in your office. Take as many security-related classes as you can. Learn everything you can pertaining to operating systems, networking, and security. Once you think your skills are fairly strong in the security realm, start studying for and take the Security+ exam.

If you have been in networking and/or security for four years or so, and you think your skills are pretty strong, consider pursuing the CISSP. After getting your CISSP, and if you’re a technical person, consider the GSEC, it complements the CISSP. The CISSP covers the 10 domains from a manager’s perspective, while the GSEC is more technical in nature within the same areas of study; policy, encryption, etc.

# Appendix B: Security Certification Ladder

IT certification programs are often organized into layers, where those at the bottom are intended to educate and prepare IT professionals to master a certain collection of skills and knowledge. At the same time, they're also intended to prepare those same professionals to "kick it up a notch" and climb up the ladder to the next level, once the current one has been explored and attained.

## Entry Level

A great many IT certification programs start with entry-level certifications because they provide gentle points of access to the overall collection of credentials a program incorporates. In many cases, large, successful IT cert programs also work with secondary (high school, mostly) and post-secondary (community colleges, technical schools, and some 4-year undergraduate programs) educational institutions to incorporate certification curriculum elements (and the skills and knowledge they capture) into broader and more general educational programs.

By design, entry-level credentials appeal to a broad spectrum of practicing and aspiring IT professionals. They're intended to stimulate interest and participation, and are generally easy to earn, while still preserving genuine value for knowledge acquired, and skills developed.

They will often define the entry points for various technical areas or specialties within a certification domain, and set the tone for what follows in more advanced areas.

## Associate Level

At the associate level, IT certification programs get more detailed and demanding.

In many professions an associate is someone who's been through basic training and who understands the fundamentals of the tools, processes, and procedures involved in working as a full-time practitioner. But an associate is also someone who needs more detailed training, particularly in the ins and outs involved in filling specific job roles, and in undertaking a variety of well-defined but necessary tasks and activities.

Ditto for IT certification programs, where associate level credentials usually define the basic skills and knowledge that junior workers will need to fill specific job roles under the supervision of a more experienced superior.

Where entry level certifications seldom provide serious or significant advantages where hiring and promotion are concerned, associate level certifications start to matter, particularly in more technical or specialized IT domains like network or systems administration, database management or programming, storage management, and so forth.

## Professional Level

At the middle of the ladder, the certification numbers begin to decline and the effort and value to obtain professional-lever certifications increase.

By the time an IT professional starts into a professional level certification, they usually have five or more years invested into their IT career, and have already acquired some meaningful on-the-job experience.

Earning a professional level IT certification can involve anywhere from 6 months to a year's worth of study, practice, and skills development, usually outside normal working hours. It can also involve some appreciable expense -- anywhere upwards of $1,000 for exams, study materials, and practice tests for those who take the self-study route; and up to three or four times that amount in programs that require classroom training (such as the VMware VCP certifications) before candidates are allowed to sit for the certification exam.

Professional level credentials can deliver appreciable value to IT professionals, both in the hiring process for new positions and in consideration for promotion or advancement in an existing job.

### Expert Level

At the expert level, difficulty goes up dramatically, and the population of those who achieve expert-level certifications goes down correspondingly.

It doesn't matter what kind of expert level certification you look into, you'll find a serious, well-qualified, and highly-trained and -experienced IT professional behind such a title. Just as the CCIE is the gold standard in the Cisco world; the Microsoft Certified Master (MCM) is emerging in that world as a counterpart, with the VCDX likewise for the VMware world, and so on.

Most such individuals have at least 10-20 years of solid working experience including significant education, technical skills and knowledge. Earning these kinds of credentials often takes 2-3 years to complete, and can involve extremely difficult examinations or reporting / documentation requirements along the way.

### Architect Level

It's only in the last 8-10 years that most certification programs have added architect or other pinnacle-level IT certifications. Climbing to the top of any IT certification heap is clearly exceptional, and remains a unique and towering achievement for those IT professionals who survive such ascents.

## Security Certification Path

Start your security certification journey with a broad, entry-level security certification. This could be one of the following credentials, any of which will provide an excellent and thorough background in computer security theory, operations, practices and policies:

### **CompTIA Security+**

CompTIA's Security+ certification has become *the* entry-level information security certification of choice for IT professionals seeking to pursue further work and knowledge in this area.

### **(ISC)² Systems Security Certified Practitioner (SSCP)**

The International Information Systems Security Certification Consortium is also home to the CISSP, the best-known senior-level security certification. Those interested in pursuing the SSCP need to possess at least one year of experience in one or more of the seven SSCP Common Body of Knowledge domains. Candidates must also pass an exam to obtain the credential. Those who do not yet meet the experience requirement may choose to first obtain the Associate of (ISC)2 certification, which is available to any candidate who passes the CAP, CCFP, CISSP, CSSLP, HCISPP or SSCP exam.

### **SANS GIAC Information Security Fundamentals Certification (GISF)**

The SANS Institute is a long-standing and well-recognized organization in the security industry. Likewise, its GIAC certifications continue to accrue visibility and acceptance. The GISF opens the door to other credentials in the respected SANS GIAC program. Since the GISF is an entry-level credential, there are no prerequisites; candidates need only pass a single exam to obtain the credential.

From here, practitioners can tackle a premium or senior-level security certification. Most such certifications require three or more years of relevant, on-the-job experience. Many also require submitting papers or research results in addition to passing exams, as well as taking specific classes.

### **CompTIA Advanced Security Practitioner (CASP)**

The CASP is intended as a follow-on to Security+ and is intended to recognize IT professionals with three or more years of direct, day-to-day information security experience, with skills and knowledge to match. The CASP requires continuing education for maintenance or a re-take of the exam every three years. It costs around $390, which is less than the CISSP, but it is ranked the same for a variety of Department of Defense-related IT positions, which will no doubt contribute to its future popularity. CompTIA announced an update to the CASP certification exam in February 2015 that includes new questions about contemporary threats as well as troubleshooting processes related to data, endpoint and network security.

### **(ISC)² Certified Information Systems Security Professional (CISSP)**

The CISSP is arguably the best-known senior-level security certification in North America. It frequently shows up in top 10 certification wish and want lists, and it is often requested by name in job postings and classified ads. Those who are interested in extending their CISSP credentials should also look into its three concentrations -- Architecture (CISSP-ISSAP), Engineering (CISSP-ISSEP) and Management (CISSP-ISSMP). The CISSP exam costs $599 with an additional fee of $399 for each of the three specialty concentration areas.

Candidates without a college degree must possess at least five years of paid professional experience to qualify for the credential; degreed individuals only need four years of paid experience. A waiver for one year of experience may be obtained (approval required) if the candidate possesses an (ISC)2 credential from an approved (ISC)2 list.

### **SANS GIAC Security Certifications**

SANS Global Information Assurance Certification offers numerous topical specializations that extend the GISF and the GIAC Security Essentials Certification (GSEC), including firewalls, incident handling, intrusion analysis, Windows and Unix administration, information security officer and systems and network auditor certifications. This is a topical, timely and highly technical program based on outstanding training online or at SANS conferences. For those willing to acquire four of these individual credentials (two of them "gold") and sit for a lengthy exam in two parts, moving on to the GIAC Security Engineer (GSE) certification probably makes sense.

### **Qualified Information Security Professional Certification**

Security University's certification requires some of the best, most intense and hands-on information security training around. Highly popular with government and industry security heavies, this program is expensive, demanding and time-consuming, but it's worth the intensive investment it requires to complete.

# Appendix C: Career Self-Assessment

Want to learn about different career pathways in cybersecurity and complete a self-assessment project to better understand the right path for you? The University of Washington offers the free course “[Finding your Cybersecurity Career Path](file:///C:/Users/A3CI/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/7GU8Q4X2/:%20https:/www.edx.org/course/cybersecurity-career-self-assessment-uwashingtonx-cyb004x)” that focuses on the pathways to cybersecurity career success.

This course is offered free of charge. In it, you will focus on the pathways to cybersecurity career success. You will determine your own incoming skills, talent, and deep interests to apply toward a meaningful and informed exploration of 32 Digital Pathways of Cybersecurity.

You will complete a self-assessment comprised of elements needed to determine essential next steps on your career path.

**What you'll learn**

By the end of this course, you will be able to:

* Understand a multitude of cybersecurity career path opportunities
* Apply problem-solving skills toward self-evaluation of compatibility with career pathways
* Narrow your exploration to the most compatible job path(s) in cybersecurity
* Assess knowledge, skills, and abilities in relation to the specific (and emerging) requirements for those paths
* Discover and identify training and other next steps needed to satisfy requirements and meet goals in cybersecurity pathways

# Appendix D: Risk Management Handbook Quick Guide

|  |  |  |
| --- | --- | --- |
| **Document** | **Key Topics** | **Version** |
| Chapter 4: Security Assessment and Authorization (CA) | Security Assessment Steps, System Interconnections, Plans of Action and Milestones (POA&M), Risk Acceptance (Risk Based Decision (RBD)), Security Authorization, Continuous Monitoring, Penetration Testing | 1.0; 1/9/2019 |
| Chapter 5: Configuration Management (CM) | Baseline Configuration, Reviews and updates, Retention of previous configurations, Systems for high risk areas, Change control*,* Security impact analysis, Separate test environments, Least functionality, Configuration Management Plan, User-installed software | 1.1; 5/3/2018 |
| Chapter 8: Incident Response (IR) | Incident Response Training, Incident Response Testing, Incident Handling, Incident monitoring, Incident Reporting, Incident Response Assistance, Incident Response Plan | 1.1; 8/7/2017 |
| Chapter 10: Media Protection (MP) | Media transport, Media Sanitization |  |
| Chapter 11: Physical and Environmental Protection (PE) | Physical access control | 1.0; 10/8/2019 |
| Chapter 12: Security and Privacy Planning (PL) | System Security Plan (SSP), Security Categorization (FIPS 199), Authorization Boundary, System Interconnection/Sharing, Security Control Selection (Common/Hybrid/System controls defined), Documenting Security Control Implementations, ATO procedure in CFACTS | 1.0; 1/31/2019 |
| Chapter 6: Contingency Planning | Contingency Planning (CP) planning requirements, Recovery metrics and terminology, disaster types, CP plan development, CP exercise , roles and responsibilities | 1.2; 1/28/2019 |
| Chapter 14: Risk Assessment | System categorization, high value assets***,*** ISRA Template, Risk Acceptance, Plan of Action and Milestones (POA&M) Guide, | 1.1; 10/29/2018 |
| Chapter 19: Privacy | HIPAA/HITECH/Privacy Act, FISMA Privacy Policy and Procedures | 1.0; 10/26/2018 |

1. From NIST SP 800.37 Rev 1 D.5, “Possesses professional qualifications, including training and experience, required to administer the information security program functions.” [↑](#footnote-ref-2)
2. See [ISSO Template](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS1223299) [↑](#footnote-ref-3)
3. See [CFACTS User’s Manual](https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx) [↑](#footnote-ref-4)
4. See [Acceptable Risk Safeguards 3.1](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication) [↑](#footnote-ref-5)
5. See [Risk Management Handbook Chapter 5 Configuration Management Version 1.2](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-05-Configuration-Management) and [Security Impact Analysis (SIA) Template Version 1.0](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/Security-Impact-Analysis-Checklist-Template) [↑](#footnote-ref-6)
6. See [Risk Management Handbook (RMH) Chapter 12: Security and Privacy Planning, Section 3.1.2](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-12-Security-and-Privacy-Planning) and [CFACTS User Manual Version 4.5 Sections 4.3.2. and 4.3.3](https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx). [↑](#footnote-ref-7)
7. See [Risk Management Handbook (RMH) Chapter 12: Security and Privacy Planning, Section 3.1.4](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-12-Security-and-Privacy-Planning) and [CFACTS User Manual Version 4.5 Sections 4.4.1 and 4.4.2](https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx) for information on authorization boundaries [↑](#footnote-ref-8)
8. See [CMS Information Security and Privacy Policy (CMS IS2P2) Version 2.0, Section 4.1.7](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Systems-Security-and-Privacy-Policy-IS2P2) for information on HVAs [↑](#footnote-ref-9)
9. See [CFACTS User Manual Section 11.3](https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx) for information on how to inherit a control [↑](#footnote-ref-10)
10. See [Acceptable Risk Safeguards Version 3.2, Sections 2, 5.1](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication) for information about non-mandatory controls [↑](#footnote-ref-11)
11. See [Risk Management Handbook (RMH) Chapter 12: Security and Privacy Planning*,* Section 3.1.7](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-12-Security-and-Privacy-Planning)

    [↑](#footnote-ref-12)
12. See [Risk Management Handbook (RMH) Chapter 12: Security and Privacy Planning](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-12-Security-and-Privacy-Planning) for information related to documentation requirements [↑](#footnote-ref-13)
13. See [CFACTS User’s Manual](https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx) [↑](#footnote-ref-14)
14. See [ISRA Template](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/Information-System-Risk-Assessment-Template) [↑](#footnote-ref-15)
15. See [CMS Privacy Impact Assessment (PIA) Standard Operating Procedures (SOP)](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Privacy-Impact-Assessment-SOP) [↑](#footnote-ref-16)
16. See [CMS Privacy Handbook Version 1.0](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Privacy-Handbook) for information about TPWA and TPWA PIAs [↑](#footnote-ref-17)
17. See [Risk Management Handbook Chapter 6 Contingency Planning FINAL](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-6-Contingency-Planning) [↑](#footnote-ref-18)
18. See [NIST Information System Contingency Plan Template](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/NIST-Information-System-Contingency-Plan-Template) [↑](#footnote-ref-19)
19. See [Risk Management Handbook Chapter 6 Supplemental CP Exercise Procedure FINAL Version1.1](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-6-Supplemental-Contingency-Planning-Exercise-Procedures) for more information [↑](#footnote-ref-20)
20. See [Risk Management Handbook (RMH) Chapter 04: Security Assessment and Authorization (CA](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-4-Security-Assessment-and-Authorization)) for detailed information about the assessment, penetration test, Risk Acceptance (Risk-Based Decision), and POAM process. [↑](#footnote-ref-21)
21. See[Adaptive Capabilities Testing (ACT) Security and Risk Assessment Handbook Document Version: 1.1 December 20, 2019](https://share.cms.gov/Office/OIT/ISPG/ACT/ISPG%20ACT%20Document%20Library/Forms/AllItems.aspx). [↑](#footnote-ref-22)
22. [See Risk Management Handbook (RMH) Chapter 04: Security Assessment and Authorization (CA](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-4-Security-Assessment-and-Authorization)) [↑](#footnote-ref-23)
23. See [Risk Management Handbook Chapter 08 Incident Response](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template) and [Risk Management Handbook Chapter 08 Incident Response Appendix K – Incident Report Template](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template) [↑](#footnote-ref-24)
24. See [HHS Information Security and Privacy Policy](https://www.hhs.gov/sites/default/files/hhs-ocio-policy-2013-0002.pdf) [↑](#footnote-ref-25)
25. See [CMS Information Security and Privacy Policy](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/POLICY_IS2P2?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending) [↑](#footnote-ref-26)
26. As of3/26/2020 [↑](#footnote-ref-27)