GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery

September 2023

CYBERSECURITY PROGRAM AUDIT GUIDE

GAO-23-104705

Accessible Version

Source: GAO; images: Who is Danny/stock.adobe.com and marinashevchenko/stock.adobe.com. | GAO-23-104705

GAO Highlights

Highlights of GAO-23-104705.

Why GAO Did This Study

GAO has long recognized the importance of information security, initially identifying it as a government-wide high-risk area in 1997. Since then, the connectivity of systems has soared, and the sophistication of attacks has rapidly escalated.

Given the urgency to address the cybersecurity threat, GAO embarked on an effort to provide guidance to analysts and auditors on conducting cybersecurity audits. Such audits are essential to identifying cybersecurity program weaknesses and developing appropriate recommendations for agency corrective actions.

The development of the CPAG reflects GAO's collective experience over the last three decades in issuing hundreds of information security and cybersecurity audit reports and making thousands of recommendations. In developing the CPAG, GAO conducted extensive outreach with internal and external stakeholders. GAO also administered a questionnaire on existing guidance and received responses from 18 federal Office of Inspectors General, five public accounting firms, and four state audit offices.

In addition, GAO held 14 focus groups with internal and external stakeholders to discuss and review key cybersecurity practices. The focus group members comprised a cross section of federal, state, and local auditors and experts as well as private and non-profit sector officials. GAO also interviewed officials from the National Institute of Standards and Technology, the Center for Internet Security, and ISACA.

View GAO-23-104705. For more information, contact Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, Vijay D'Souza at (202) 512-7650 or DsouzaV@gao.gov, or Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

September 2023

CYBERSECURITY PROGRAM AUDIT GUIDE

Why GAO Developed This Guide

The Cybersecurity Program Audit Guide (CPAG) is to be used in conducting cybersecurity performance audits. The intent of the guide is to arm cyber analysts and auditors with a set of methodologies, techniques, and audit procedures to evaluate components of agency cybersecurity programs and systems. GAO welcomes federal and other governmental organizations to use this guide to assess their cybersecurity programs.

The CPAG has six primary components:

The Cybersecurity Program Audit Guide's Six Primary Components

Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com. | GAO-23-104705

- **Asset and risk management**: developing an understanding of the cyber risks to assets, systems, information, and operational capabilities.
- **Configuration management**: identifying and managing security features for system hardware and software and controlling changes to the configuration.
- **Identity and access management**: protecting computer resources from modification, loss, and disclosure by limiting authorized access.
- **Continuous monitoring and logging**: maintaining ongoing awareness of cybersecurity vulnerabilities and threats to an organization's systems.
- **Incident response**: taking action when security incidents occur.
- **Contingency planning and recovery**: developing contingency plans and executing successful restoration of capabilities.

Each of the above components has four to seven overall key practices. For each of these practices, the CPAG provides further specificity on control objectives, applicable criteria, and available audit procedures.

Although the CPAG provides suggested approaches for addressing key cybersecurity topics, it is intended to be used in a flexible manner. Depending on audit objectives and the relative importance of specific issues, organizations may adjust and fine tune audit techniques as appropriate.

Contents

Abbreviations

BOD	binding operational directives
CDM	continuous diagnostics and mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CPAG	Cybersecurity Program Audit Guide
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
ED	emergency directive
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
GAGAS	generally accepted government auditing standards
Green Book	Standards for Internal Control in the Federal Government
HSPD	Homeland Security Presidential Directive
IDS	intrusion detection system
IPv6	internet protocol version 6
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	personally identifiable information
POA&M	plan of actions and milestones
STIGS	security technical implementation guides
VoIP	voice over internet protocol
Yellow Book	Government Auditing Standards

Preface to Cybersecurity Program Audit Guide 1.0

GAO is pleased to announce the issuance of new guidance, the Cybersecurity Program Audit Guide (CPAG), for conducting cybersecurity performance audits. GAO's intent in developing this guide is to provide cyber analysts and auditors with a set of methodologies, techniques, and audit procedures to evaluate components of agency cybersecurity programs.

Cybersecurity threats continue to rise as system connectivity increases and attack techniques grow in sophistication. Given the increasing threats, GAO initiated an effort to provide guidance to analysts and auditors on conducting cybersecurity audits. Such audits are essential to identifying cybersecurity program weaknesses and developing appropriate recommendations for agency corrective actions. Implementation of these recommendations can then lead to reduced risk of successful attacks.

GAO welcomes federal and other governmental organizations to use this guide, as appropriate, to assess their cybersecurity programs. In doing so, organizations may need to modify or tailor techniques depending on their specific objectives.

GAO wants to thank the many organizations and individuals who contributed to the development of this guide. Special thanks to several organizations who provided invaluable input to the development of this guide, including the National Institute for Standards and Technology, the Center for Internet Security, ISACA, federal and state auditors, and several professional auditing organizations and independent public accounting firms for their significant input to the development of this guide (see app. III). GAO wants to thank everyone involved for sharing their insights, experience, and time.

Nick Marin

Nick Marinos
Managing Director,
Information Technology and Cybersecurity,
U.S. Government Accountability Office

Vijay A. D'Souza

Vijay A. D'Souza
Director,
Information Technology and Cybersecurity,
U.S. Government Accountability Office

Jennifer R. Franks,
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity,
U.S. Government Accountability Office

Addressing Cybersecurity Is an Urgent Priority

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information.[1] The security of these systems and data is vital to public confidence and national security, prosperity, and well-being. Many of these systems contain vast amounts of personally identifiable information (PII), thus making it imperative to protect the confidentiality, integrity, and availability of this information and effectively respond to data breaches and security incidents when they occur.[2]

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated. These risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks.

In particular, foreign nations—where adversaries may possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks. Rapid developments in new technologies, such as artificial intelligence and the Internet of Things, makes the threat landscape even more complex and can also potentially introduce security, privacy, and safety issues that were previously unknown.[3]

Compounding these risks, IT systems are often riddled with security vulnerabilities—both known and unknown. These vulnerabilities can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety. This is illustrated by the over 32,000 significant security incidents at federal agencies reported by the Cybersecurity and Infrastructure Security Agency (CISA) in fiscal year 2021, including almost 18,000 breaches involving PII.[4]

Legislation, executive branch guidance, and policy documents emphasize the importance of cybersecurity for federal agencies. For example, the *Federal Information Security Modernization Act of 2014* (FISMA), and its predecessor, the Federal Information Security Management Act of 2002, established a comprehensive framework of guidelines and security standards to protect government information systems and programs.[5] The law requires, among other things, that agencies report annually on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprises. Additionally, in May 2017 the President issued Executive Order 13800, requiring agencies to begin using the National Institute of Standards and Technology (NIST's) Cybersecurity Framework for managing their cybersecurity risks.[6] Further, the Office

[1] GAO, *High-Risk Series: An Update,* GAO-03-119 (Washington, D.C.: January 2003).

[2] PII refers to any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, or biometric records, and any other information which is linked or linkable to an individual. Any information that can be used to distinguish or trace an individual's identity is potentially PII.

[3] Internet of Things technology refers to devices collecting information, communicating it to a network and, in some cases, completing a task—like unlocking doors using a smartphone application.

[4] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2021* (Washington, D.C.: Sept. 14, 2022).

[5] The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this publication, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[6] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: April 2018).

of Management and Budget (OMB) has issued additional guidance to help agencies, such as OMB A-130 and FISMA reporting requirements.[7] In May 2021, the President issued Executive Order 14028. The order requires the Department of Homeland Security's CISA, NIST, and executive branch agencies to take significant action at every level to improve areas such as increasing threat information sharing, modernizing federal government cybersecurity, enhancing software supply chain security, and improving the federal government's detection and handling of threats and vulnerabilities.[8]

To highlight the importance of these issues, we have designated information security as a government-wide high-risk area since 1997.[9] In 2003, we expanded our high-risk area to include critical infrastructure. This consists of the nation's critical physical and cyber assets and systems—such as energy, transportation, communications, and financial services— that are so vital to the United States that their incapacity or destruction could have a debilitating impact on national security, public health and safety, or the economy.[10] Organizations that own or operate critical infrastructure have increasingly sought to gain efficiencies by connecting their physical and cyber systems, and the convergence between these assets and systems creates new opportunities for potential attackers.[11]

In 2015, we also added protecting the privacy of PII to this high-risk area.[12] Since then, advances in technology have enhanced the ability of government and private sector entities to collect and process extensive amounts of PII, which has posed challenges to ensuring the privacy of such information. In addition, high-profile PII breaches at commercial entities, such as Equifax, heightened concerns that personal privacy is not being adequately protected.

In our high-risk updates from September 2018 and March 2023, we emphasized the critical need for the federal government to take 10 specific actions to address four major cybersecurity challenges that the federal government faces.[13] These challenges are (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. These challenges and action items are shown in figure 1.

[7] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

[8] The White House, *Executive Order on Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[9] GAO, *High-Risk Series: Information Management and Technology*, HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Overview*, HR-97-1 (Washington, D.C.: February 1997).

[10] GAO-03-119.

[11] The term "critical infrastructure" as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. §5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

[12] GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[13] GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to be Maintained and Expanded to Fully Address All Areas,* GAO-23-106203 (Washington, D.C.: Apr. 20, 2023), and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

Figure 1: Four Major Cybersecurity Challenge Areas

Establishing a comprehensive cybersecurity strategy and performing effective oversight

1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

3 Address cybersecurity workforce management challenges.

4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5 Improve implementation of government-wide cybersecurity initiatives.

6 Address weaknesses in federal agency information security programs.

7 Enhance the federal response to cyber incidents.

Protecting cyber critical infrastructure

8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

9 Improve federal efforts to protect privacy and sensitive data.

10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis; images: GAO, peshkov/stock.adobe.com, Gorodenkoff/stock.adobe.com, metamorworks/stock.adobe.com and Monster Ztudio/stock.adobe.com. | GAO-23-104705

Developing the Guide

Given the increasing criticality of cybersecurity, our objective was to develop a revised guide for conducting performance audits of relevant components of agency cybersecurity programs. To begin this process, we began by gathering feedback on the existing Federal Information System Controls Audit Manual (FISCAM).[14]

First, we developed and administered a questionnaire to existing FISCAM users. Our questions focused on FISCAM's current composition, organization, applicability, usefulness, and areas of possible improvements. We received responses from numerous users, including 18 federal Office of Inspectors General, five independent public accounting firms, and four state audit offices.

Based on our analysis of the responses, we generated questions for subsequent focus group discussions. We then held 10 focus groups with internal and external stakeholders and users to discuss FISCAM. The focus groups included senior executives, managers, and analysts across GAO; Office of Inspectors General; Independent Public Accounting representatives; and state auditors. Further, we interviewed officials from NIST, the Center for Internet Security, and ISACA, among others.[15]

We then performed a content analysis of the focus group and interview results. The most frequently identified suggestions were shortening FISCAM, clarifying which portions of the manual were most important to perform, aligning FISCAM to current NIST frameworks and federal guidance, and keeping FISCAM up to date.

As a result of this feedback, we determined we would both update FISCAM and develop this new Cybersecurity Program Audit Guide or CPAG.[16] The FISCAM update will continue to address financial audits, including financial statement and related internal control audits, and attestation engagements. The CPAG is to be used on performance audits of key components of agency cybersecurity programs.

The CPAG addresses many of the comments discussed above. For example, it has been significantly streamlined to slightly less than 100 pages. Additionally, the scope of the guide is performance audits of key components of agency cybersecurity programs. Relative to our prior graphic on the four cybersecurity challenge areas and 10 action items, the guide can be applied to multiple areas, but would likely most frequently apply to the action item of addressing weaknesses in federal agency cybersecurity programs. It could apply to other action items as well, such as:

- enhancing the federal response to cyber incidents,
- improving federal efforts to protect privacy and sensitive data, and
- mitigating global supply chain risks.

The CPAG relies heavily on existing guidance. Specifically, we use many of the practices covered by NIST Special Publication (SP) 800-53 Revision 5, the NIST Cybersecurity Framework, and other related NIST guidance; OMB cybersecurity control-related policies and guidance; and industry leading practices, such as Center for Internet Security controls. The guide incorporates, as appropriate, additional sources of relevant criteria and audit procedures.

[14] GAO, *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G (Washington, D.C.: February 2009).

[15] The non-profit Center for Internet Security focuses on helping safeguard public and private organizations against cyber threats.

[16] GAO, *Federal Information System Controls Audit Manual* (FISCAM) 2023 Exposure Draft, GAO-23-104975 (Washington, D.C.: July 2023).

References to NIST and other organizations in this guide do not imply endorsements of this guide.

As part of this process, we convened four working groups of knowledgeable specialists to review and discuss the draft of leading practices, relevant criteria, and audit procedures. Group members represented government organizations, private companies, independent consultant groups, and trade industry groups throughout the U.S. See appendix III for a list of the 49 work group participants.

We sent the full draft CPAG to other external stakeholders and asked them to review the chapters and provide us with feedback. In addition, we asked for review and comments from stakeholders across GAO on draft chapters. We made changes, as appropriate, throughout the guide to reflect these comments. In considering the comments received, we also relied on the experience of our senior IT and cybersecurity leaders, managers, and analysts. Collectively, over the last three decades, we have issued hundreds of cybersecurity and information security reports and testimonies, and made thousands of related recommendations.

We conducted our work from January 2021 to September 2023 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for the guidance in this product.

How to Use this Guide

This guide provides guidelines and illustrative examples of audit procedures that can be used to perform a review of relevant components of a U.S. federal government agency's cybersecurity program. Other audit organizations may also find this guide helpful. As a guide, the CPAG is not a required auditing standard such as the Yellow Book. Therefore, the use of "should" statements in this guide do not indicate a requirement unless explicitly stated in criteria. The guidelines are resource intensive and, as such, it is likely not feasible or necessary to assess the effectiveness of all cybersecurity controls within an IT system for each audit. In addition, the control techniques sufficient to achieve a particular objective will vary depending on the risk and the audit objectives. The CPAG is not intended to list every possible control objective and audit procedure that may be appropriate. Therefore, an auditor should apply professional judgment to determine the extent that additional and more detailed audit steps and tailored control activities are needed based on the organization being audited, the audit objectives, and key areas of audit interest.

This guide contains control activities that are consistent with those in NIST SP 800-53 Revision 5 and other NIST and OMB cybersecurity control-related policies and guidance.

Additional nongovernmental sources are available for use in conducting cybersecurity audits.[17] Further, if an engagement is focused on national security systems, auditors should also use the specific criteria that apply to those systems. We suggest users review the Committee on National Security Systems Instruction, which may be accessed at https://www.cnss.gov/cnss/, for more information.
The chapters in this guide are organized as follows: Chapter 1 is a general guide to the audit process and the main phases of a performance audit focused on cybersecurity. Chapters 2 to 7 provide details on the six main components to consider when conducting a comprehensive cybersecurity audit.

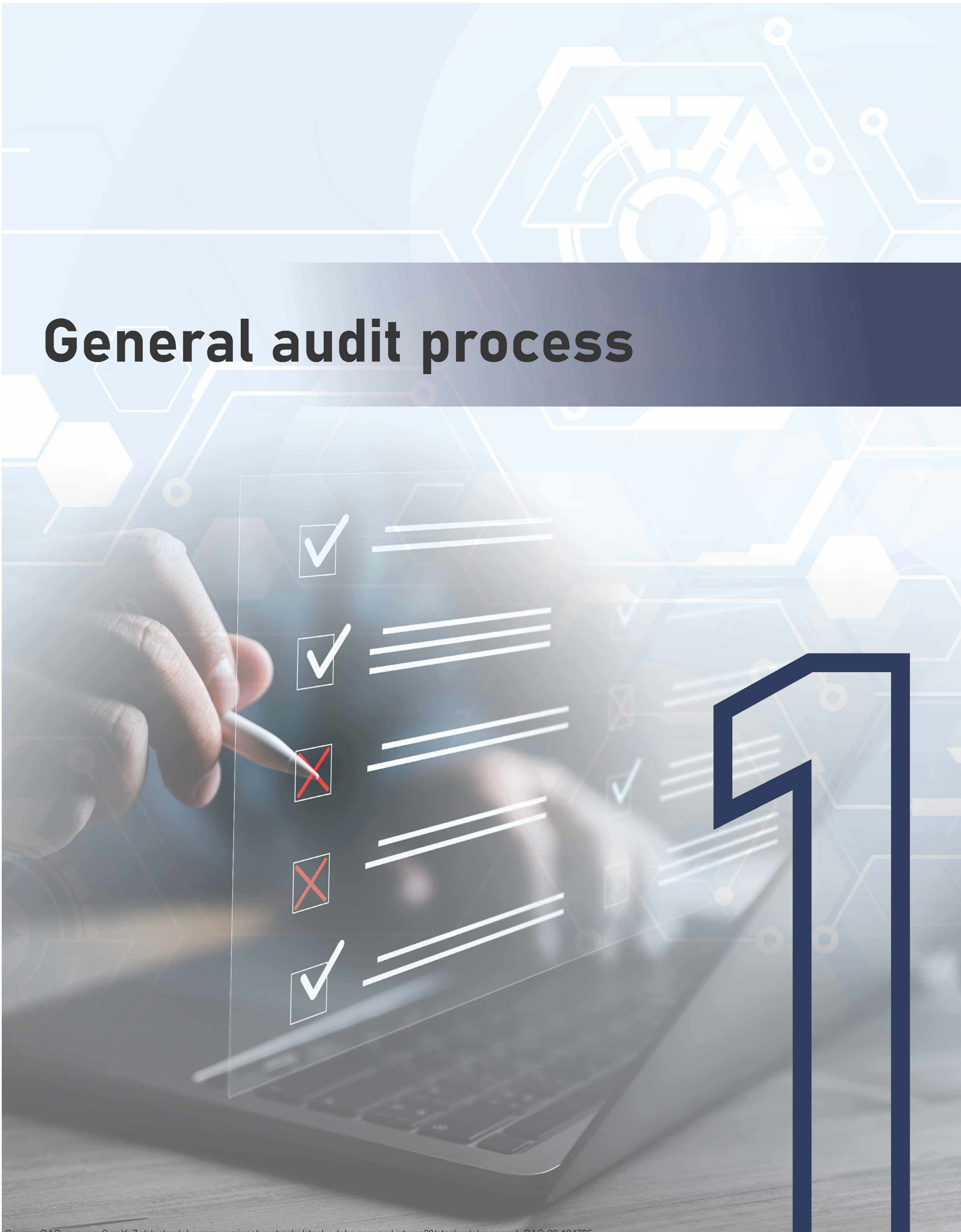
- Chapter 2 covers asset and risk management—developing an organizational understanding of the cyber risks to assets, systems, information, and operational capabilities.
- Chapter 3 addresses configuration management—identifying and managing security features for system hardware, software, and firmware; and controlling changes to the configuration.
- Chapter 4 deals with identity and access management—protecting computer resources from modification, loss, and disclosure by limiting authorized access and detecting unauthorized access.
- Chapter 5 covers continuous monitoring and logging—maintaining ongoing awareness of cybersecurity vulnerabilities and threats to an organization's systems and networks.
- Chapter 6 addresses incident response—taking action when actual or potential security incidents occur.
- Chapter 7 discusses contingency planning and recovery—developing contingency plans and executing successful restoration of capabilities.

Chapters 2 through 7 each contain a list of key criteria to consider. The criteria listed are not an exhaustive or all-inclusive list of possible criteria. Further, the criteria listed are current as of the time of this guide's publication. Prior to using the criteria, auditors should make sure they are using the most current version and consider use of additional criteria as appropriate.

[17] For example, MITRE D3FEND is a complimentary cybersecurity framework developed in coordination with the National Security Agency that is intended to address the implementation of defensive techniques by both governmental and private organizations. Another example is the CIS critical security controls which are a set of 18 cybersecurity controls that provide key actions to block or mitigate cybersecurity attacks.

General audit process

1



Source: GAO; images: SomYuZu/stock.adobe.com, marinashevchenko/stock.adobe.com and ixtumz88/stock.adobe.com. | GAO-23-104705

Chapter 1. Cybersecurity Program Audit Process

The CPAG is based on generally accepted government auditing standards and systemic processes that GAO uses for performance audits. The professional standards presented in the 2018 revision of Government Auditing Standards (known as the Yellow Book) provide a framework for performing high-quality audit work with competence, integrity, objectivity, and independence to provide accountability and to help improve government operations and services.[18] These standards, commonly referred to as generally accepted government auditing standards or GAGAS, provide the foundation for government auditors to lead by example in the areas of independence, transparency, accountability, and quality through the audit process.

According to GAGAS, performance audits provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight. These audits can, among other things, improve program performance and operations, reduce costs, facilitate decision-making by parties responsible for overseeing or initiating corrective action, and contribute to public accountability. Performance audit objectives vary widely and include assessments of program effectiveness, economy, and efficiency; internal control; compliance; and prospective analyses. Audit objectives may also pertain to the current status or condition of a program. These overall objectives are not mutually exclusive. For example, a performance audit with an objective of determining or evaluating program effectiveness may also involve an additional objective of evaluating the program's internal controls. Further descriptions of key categories of performance objectives follow:

- **Program effectiveness and results audit objectives.** These often focus on program results and may measure the extent to which a program is achieving its goals and objectives.

- **Economy and efficiency objectives.** These address, among other things, the costs and resources used to achieve program results.

- **Internal control audit objectives.** These relate to an assessment of one or more aspect of an organization's system of internal control that is designed to provide reasonable assurance of achieving effective and efficient operations, reliability of reporting for internal and external use, or compliance with provisions of applicable laws and regulations. Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity.

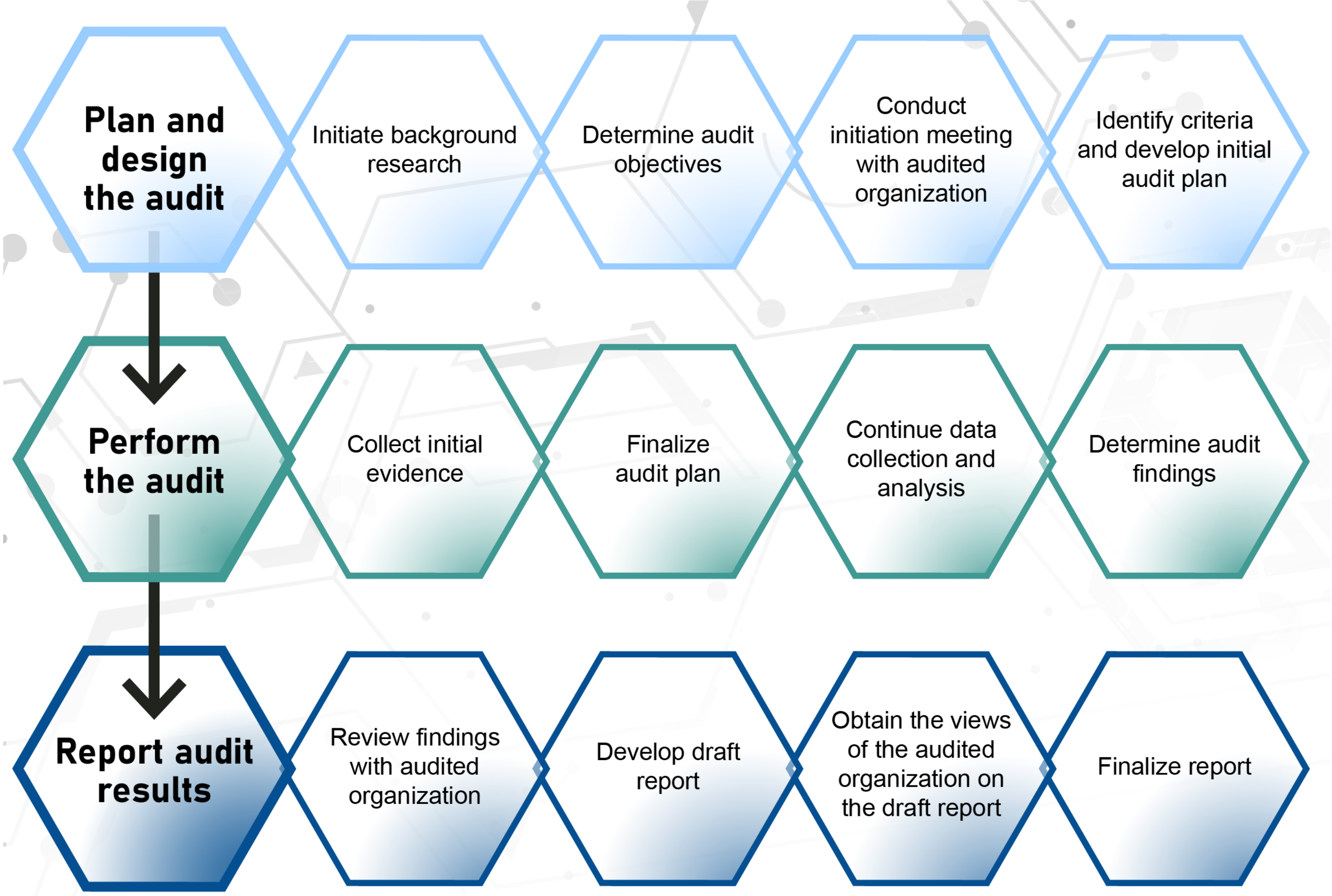
Fieldwork requirements in GAGAS establish an overall approach for auditors to apply in planning and performing an audit to obtain sufficient, appropriate evidence that provides a reasonable basis for findings and conclusions based on the audit objectives. The fieldwork requirements for performance audits relate to planning the audit; conducting the engagement; supervising staff; obtaining sufficient, appropriate evidence; and preparing audit documentation.

Finally, GAGAS reporting requirements establish the auditor's overall approach for communicating the results of a performance audit. Reporting standards for performance audits include format, content, findings, conclusions, and recommendations.

The three main phases of a cybersecurity audit—planning and designing, performing, and reporting—are outlined in figure 2. Although each phase and the associated key activities are discussed sequentially, in reality many of the activities can overlap during an audit.

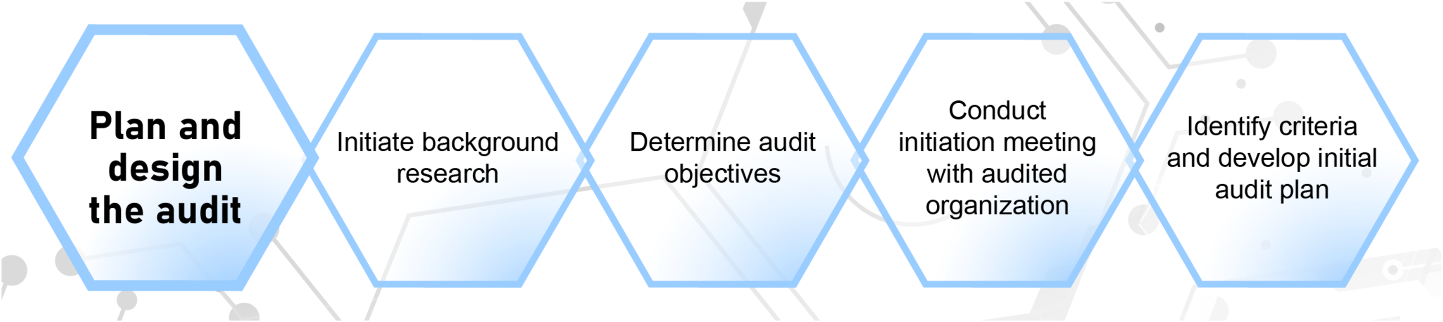
[18] GAO, *Government Auditing Standards*, 2018 Revision, GAO-21-368G (Washington, D.C.: April 2021).

Figure 2: Three Main Audit Phases


Plan and design the audit
Initiate background research
Determine audit objectives
Conduct initiation meeting with audited organization
Identify criteria and develop initial audit plan
Perform the audit
Collect initial evidence
Finalize audit plan
Continue data collection and analysis
Determine audit findings
Report audit results
Review findings with audited organization
Develop draft report
Obtain the views of the audited organization on the draft report
Finalize report

Source: GAO. | GAO-23-104705

1.1 Plan and Design the Audit


Plan and design the audit
Initiate background research
Determine audit objectives
Conduct initiation meeting with audited organization
Identify criteria and develop initial audit plan

Source: GAO. | GAO-23-104705

Planning is a key part of every audit. Adequate planning helps to address the audit objectives, design the methodology to obtain sufficient evidence, reduce audit risk to an acceptably low level, and provide a reasonable basis for findings and conclusions based on the audit objectives. During the planning phase, it is important to (1) initiate background research, (2) determine audit objectives, (3) conduct an initiation meeting with the audited organization, and (4) identify criteria and develop an initial audit plan.

1.1.1 Initiate Background Research

Prior to engaging with the audited organization, gaining an understanding of that organization can help inform the planning phase. Information relevant to the engagement can be obtained by reviewing prior audit work and other sources of publicly available information (e.g., organization’s website, organizational charts, policy documents, prior audit reports, and relevant published articles). Of particular importance is reviewing previously issued relevant reports and associated recommendations.

1.1.2 Determine Audit Objectives

Developing and documenting the cybersecurity audit objectives are essential to the audit. The objectives are what the audit is intended to accomplish. Audit objectives can be viewed as questions that auditors seek to answer based on evidence obtained and assessed against criteria. Audit objectives may also pertain to the current status or condition of a program.[19] Objectives, scope, and methodology may be adjusted as the work is performed.[20] Objectives may include:

- supporting an evaluation of cybersecurity controls as required by FISMA and other relevant legislation;[21]
- supplementing performance audits by assessing the effectiveness of cybersecurity within the context of a broader systems review;
- supporting other performance audits, such as assessing data reliability or how well an information system protects the confidentiality, integrity, and availability of data;

[19] The term program as used in GAGAS includes processes, projects, studies, policies, operations, activities, entities, and functions.

[20] Scope is the boundary of the audit and is directly tied to the audit objectives. The methodology describes the nature and extent of audit procedures for gathering and analyzing evidence to address the audit objectives.

[21] 44 U.S.C. §3554(2)(D).

- determining the effectiveness of cybersecurity controls and identifying any risks related to how they are implemented; and
- examining the system development processes and procedures.

Determine Audit Scope and Boundaries

Scope represents the boundaries of the audit and is directly tied to the audit objectives. The scope defines the subject matter that the auditors will assess, such as a particular program or aspect of a program, the necessary documents or records, the period of time reviewed, and the locations that will be included. The scope of a cybersecurity audit involves deciding on the IT systems, functionality, and processes to be assessed. It may also include determining the policies and procedures to be covered. For example, the scope may:

- comprehensively address an entire organization, a component, or a network, or may narrowly target an application, specific technology (e.g., wireless, cloud, blockchain, and artificial intelligence), or location (e.g., systems or applications managed by other entities); and/or
- include all controls or only a selected number of controls within a category such as configuration management.

In scoping the audit, prioritizing key assets of interest is important. The criteria used to prioritize the systems should reflect the audit objectives. For example, if the objective is to assess an organization’s most critical IT systems, an auditor should consider prioritizing systems of interest based on their Federal Information Processing Standards (FIPS) 199 impact ratings and designations as high-value assets. Determining which cybersecurity controls and control assessment methods are relevant to the audit objectives and are necessary to achieve the control activities is essential. If the scope is constrained due to limited time or resources, the focus should be on the organization’s highest risk and highest priority items.

Furthermore, prior to scoping the audit, consideration should be given to the operational environment of the audited organization. This is particularly important if some or all of the organization’s systems operate in the cloud. The shift to cloud services—whether that service be infrastructure, platform, or software—may impact the extent to which the auditor can assess certain aspects of an organization’s IT systems and network.

Finally, the audit organization’s management should ensure that the audit team collectively has the requisite skills to conduct the audit. For example, the team should have sufficient, specialized technical knowledge to evaluate the technologies and systems that are within the audit scope.

1.1.3 Conduct Initiation Meeting with Audited Organization

The audit team should conduct an initial meeting with the audited organization to inform it of objectives, preliminary scope and methodology, and expected time frames. At this initial meeting, a request should be made of the organization to provide relevant documents. Based on objectives, aspects of the following general information may be requested:

- **Mission and business processes.** Obtain documents describing how the business processes relevant to the audit objectives enable the organization to fulfill its mission, and the extent to which those processes are dependent upon IT systems and infrastructure. Examples of evidence to request include collecting the organization’s standard operating procedures, flowcharts, and process diagrams.
- **Organizational IT structure, management, and functions.** Obtain documents on key IT-related organizational components and teams, such as those dedicated to cybersecurity protection, incident response, and the assessment and authorization process. Examples of evidence to request include organizational charts, cybersecurity and privacy policies, and applicable procedures.

- **Budget and funding**. Obtain documents on IT and cybersecurity expenditures. Examples of evidence to request include the organization's IT and cybersecurity budget requests, and reports showing actual expenditures.

- **Personnel and locations.** Obtain documents on the size and composition of the IT and cybersecurity organizations in terms of employees, contractors, and locations. Examples of evidence to request include facility security plans, applicable contracts, and documents on agency and contractor responsibilities.

- **Network and system architecture.** Obtain documents on the organization's overall network architecture, the architectures of the systems relevant to the audit, interconnections outside the organization's network, and the security and privacy controls expected to be in place.[22] Examples of evidence to request include the organization's network diagrams, an inventory of applicable systems, and system security plans and organizational security control inheritance guide.

- **Recent events and previous audits.** Obtain documents on key recent events, such as major IT and cybersecurity incidents, congressional hearings, or reorganizations that affected the organization. Examples of evidence to request include recent audit reports, congressional testimony, and internal cybersecurity assessments.

In addition to requesting general relevant documentation, an auditor should seek information on the specific networks, systems, data, and other components of the organization's cybersecurity program that are relevant to the audit objectives.[23] For example, depending on audit objectives, information may be requested on key systems/assets such as

- physical location(s) where the system is being utilized and for what purpose;

- significant components of the associated hardware (e.g., servers) and software (e.g., firewalls, routers, host configurations, and operating systems);

- systems that provide significant support (e.g., general support systems) and system interconnections, particularly those outside the organization; and

- any known vulnerabilities, recent audit findings and recommendations, and recent cybersecurity incidents.

If included in the audit's objectives, other important aspects of the organization's cybersecurity program could include user access, data access, system configurations, application controls, and other program elements. Accordingly, requesting available documentation on the organization's policies, procedures, and management of these topics would be essential.

In addition, privacy considerations may be relevant to the audit objectives since federal agencies often use IT systems and electronic data to process, maintain, and report PII. When an information system processes PII, the organization's information security program and privacy program have a shared responsibility for managing the risks to individuals that may arise from unauthorized system activity or behavior.

[22] According to NIST, a system-specific control is a security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system, a common control is a security or privacy control that is inherited by multiple information systems or programs, and a hybrid security control is implemented in part as a common control and in part as a system-specific control.

[23] This section is not intended to be used to audit business process controls.

1.1.4 Identify Criteria and Develop Initial Audit Plan

Criteria identify the required or desired state or expectation with respect to the program or operation. They provide a context for evaluating evidence and understanding the findings, conclusions, and recommendations in the report. Criteria include laws, regulations, policy and guidance that are relevant to IT at the organization, technically developed standards, and leading practices. Such laws, regulations, and guidance may establish general or specific IT control requirements or criteria. Examples of criteria and standards generally relevant to cybersecurity audits of federal agencies include FISMA requirements, the NIST risk management framework, NIST SP 800-53, the Cybersecurity Framework, Presidential Executive Order 14028, and NIST *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.*[24]

FISMA Requirements

As stated earlier, FISMA, among other things, provides a comprehensive framework to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. The law requires agencies to submit inventories of their major information systems to OMB and to report annually on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise. Specifically, FISMA states that the head of each agency shall, among other things, be responsible for ensuring that the agency

- provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;
- institutes information security management processes that are integrated with agency strategic, operational, and budgetary planning processes;
- implements information security policies and practices as required by standards and guidelines, issued in accordance with law and as directed by the President;
- assesses the risk and magnitude of the harm resulting from compromised information or information systems and determining the levels of information security appropriate to protect such information and information systems; and
- conducts periodic testing and evaluation of information security policies, procedures, and practices.

Further, FISMA requires that the inspector general or independent external auditor for each agency annually perform an independent evaluation to determine the effectiveness of the information security policies, procedures, and practices supporting their agency’s information security programs.[25] Agencies are to include the results of the evaluations in annual reports that they are required to submit to OMB, certain congressional committees, and the Comptroller General. Further, OMB is required to summarize the results in annual reports to Congress.

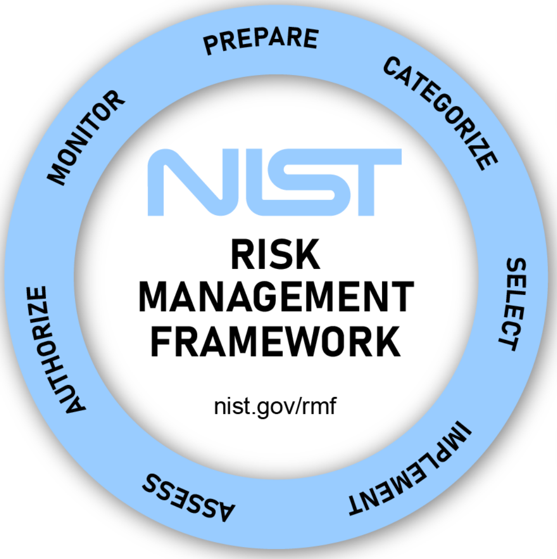
[24] National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,* SP 800-161, Revision 1 (Gaithersburg, MD: May 2022).

[25] The annual inspector general FISMA metrics and reporting instructions are developed as a collaborative effort among OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The metrics provide reporting requirements across key areas to be addressed in the independent assessment of agencies’ information security programs.

NIST Risk Management Framework

NIST developed the risk management framework to provide a process that integrates security, privacy, and cyber supply chain risk management into the system development lifecycle. The framework can be applied to new and legacy systems, any type of system or technology, and within any type of organization regardless of size or sector. See figure 3 for a summary of the major elements of the risk management framework.

Figure 3: Major Elements of the National Institute of Standards and Technology's (NIST) Risk Management Framework



Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

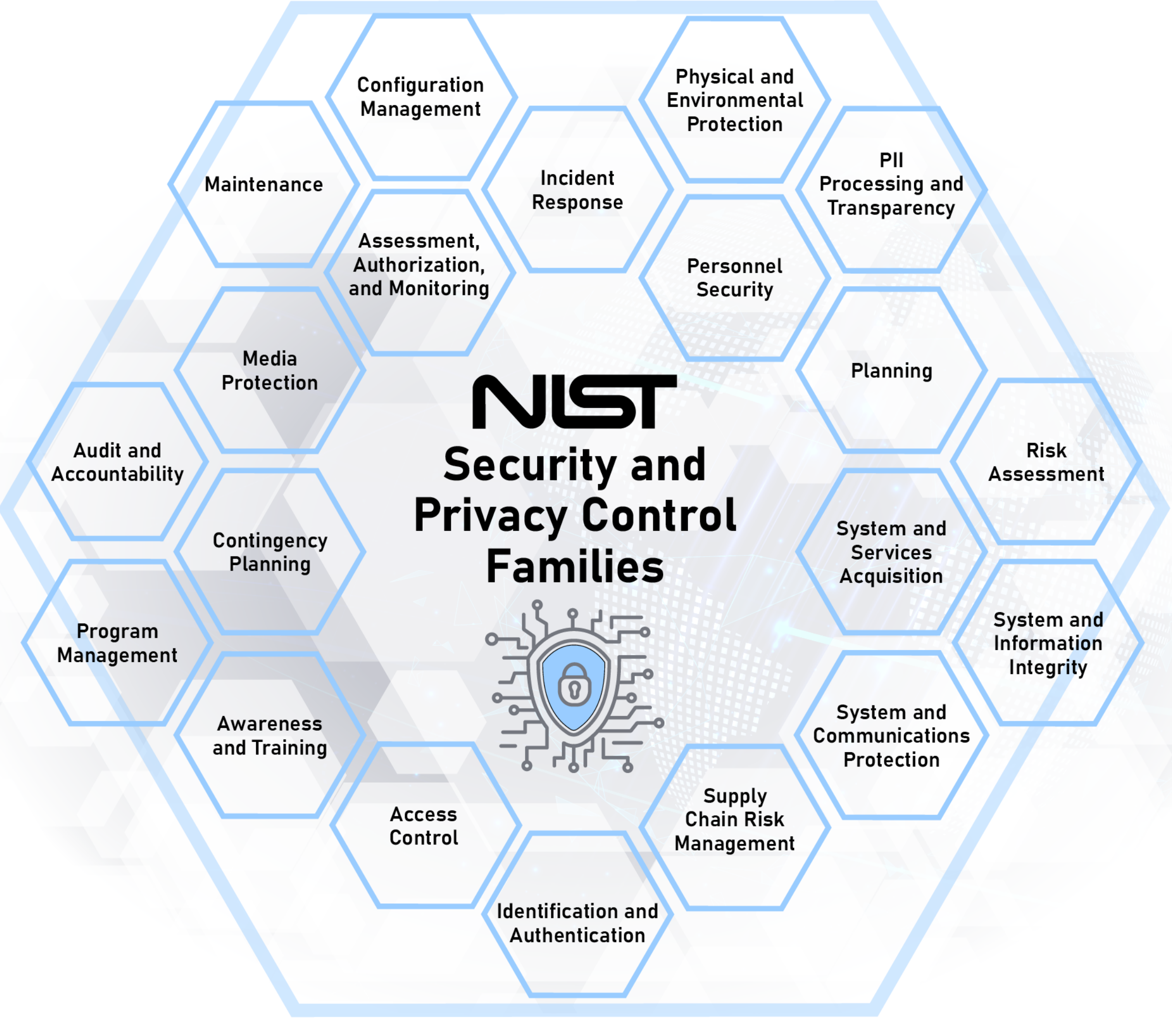
Source: *National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2,* SP-800-37 (Gaithersburg, MD: Dec 2018); images: agency logos. | GAO-23-104705

NIST SP 800-53

NIST 800-53 provides a catalog of security and privacy controls for information systems and organizations. These controls are to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.[26] SP 800-53 includes baseline security controls for low-, moderate-, and high-impact systems. Further, federal organizations have the ability to tailor or supplement their security requirements and policies based on agency mission, business requirements, and operating environment. In addition, the controls address requirements derived from laws, executive orders, directives, regulations, policies, standards, and guidelines. Further, SP 800-53 is periodically revised to incorporate new technologies and address changing threats. See figure 4 for the SP 800-53 security and privacy control families.

[26] Security control topics, referred to as families of security controls, covered by SP 800-53 include access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Figure 4: National Institute of Standards and Technology's (NIST) SP 800-53 Security and Privacy Control Families


NIST
Security and Privacy Control Families
Configuration Management
Physical and Environmental Protection
Maintenance
Incident Response
PII Processing and Transparency
Assessment, Authorization, and Monitoring
Personnel Security
Media Protection
Planning
Audit and Accountability
Risk Assessment
Contingency Planning
System and Services Acquisition
Program Management
System and Information Integrity
Awareness and Training
System and Communications Protection
Access Control
Supply Chain Risk Management
Identification and Authentication

Source: NIST; images: agency logo, marinashevchenko/stock.adobe.com and SergeyBitos/stock.adobe.com. | GAO-23-104705

SP 800-53 also addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that IT products and the systems that rely on those products are sufficiently trustworthy. Although NIST SP 800-53 applies to U.S. government systems and organizations, the federal government has made compliance with NIST SP 800-53 standards applicable to many contractors.[27]

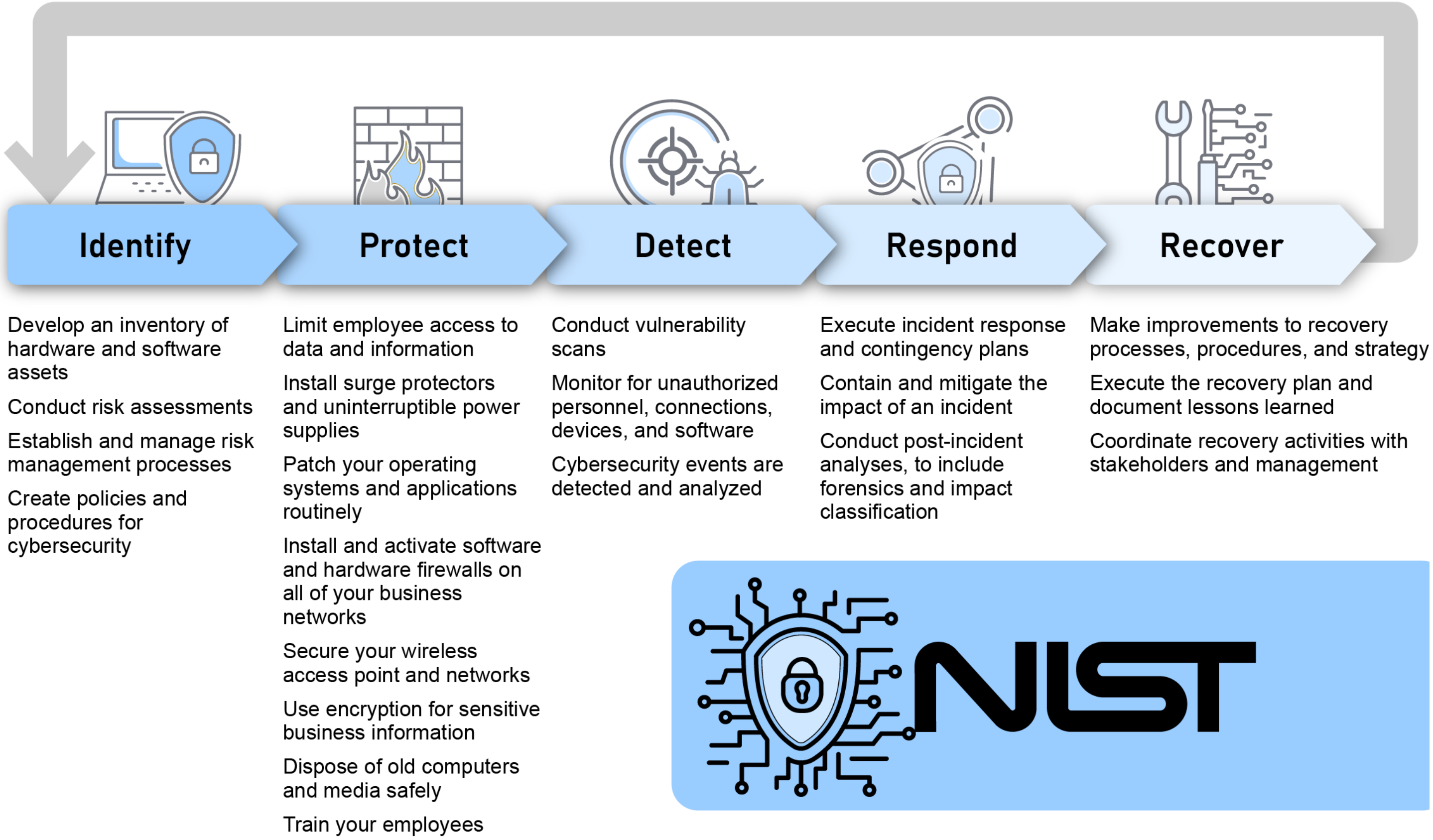
Further, NIST published SP 800-53A as a supplement to SP 800-53 to help organizations ensure that their information systems and controls are in compliance with the requirements in SP 800-53. SP 800-53A includes information on the types of assessments that can be performed, the processes and procedures for conducting assessments, and the reporting requirements for the results of those assessments.

[27] NIST SP 800-171 establishes a derived set of cybersecurity standards for contractors.

NIST Cybersecurity Framework

The Cybersecurity Framework is guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It is composed of the framework core, the implementation tiers, and the profiles. The Cybersecurity Framework has five core functions that include 23 categories and 108 subcategories. According to NIST, an organization can use its current processes and leverage the Cybersecurity Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk. Figure 5 presents a visual depiction of the Cybersecurity Framework core functions and categories.[28]

Figure 5: National Institute of Standards and Technology (NIST) Cybersecurity Framework Five Core Functions and Categories



Identify

- Develop an inventory of hardware and software assets
- Conduct risk assessments
- Establish and manage risk management processes
- Create policies and procedures for cybersecurity

Protect

- Limit employee access to data and information
- Install surge protectors and uninterruptible power supplies
- Patch your operating systems and applications routinely
- Install and activate software and hardware firewalls on all of your business networks
- Secure your wireless access point and networks
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

Detect

- Conduct vulnerability scans
- Monitor for unauthorized personnel, connections, devices, and software
- Cybersecurity events are detected and analyzed

Respond

- Execute incident response and contingency plans
- Contain and mitigate the impact of an incident
- Conduct post-incident analyses, to include forensics and impact classification

Recover

- Make improvements to recovery processes, procedures, and strategy
- Execute the recovery plan and document lessons learned
- Coordinate recovery activities with stakeholders and management

Source: GAO analysis of National Institute of Standards and Technology guidance; images: agency logo and marinashevchenko/stock.adobe.com. | GAO-23-104705

The core functions and functional areas defined in the above framework can be mapped to NIST controls outlined in NIST SP 800-53.

[28] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: April 2018). At the time of this publication NIST had initiated a process to update the NIST Cybersecurity Framework to 2.0.

NIST Privacy Framework

The NIST Privacy Framework was developed to help organizations reduce privacy risks.[29] According to the NIST Privacy Framework, although managing cybersecurity risk contributes to managing privacy risk, it is not sufficient because privacy risks can also arise by means unrelated to cybersecurity incidents. Having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. In addition to the NIST Privacy Framework, the privacy baseline within NIST 800-53 may also be used.

NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

NIST developed this publication to provide guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain.[30] According to NIST, cybersecurity risks throughout the supply chain refers to the potential for harm or compromise that arises from the cybersecurity risks posed by suppliers, their supply chains, and their products or services. Supply chain cybersecurity vulnerabilities may lead to persistent negative impacts on an organization, ranging from a reduction in service levels leading to customer dissatisfaction to the theft of intellectual property or the degradation of critical mission and business processes. Vulnerabilities in the supply chain are often interconnected and may expose organizations to cascading cybersecurity risks.

Additional Sources of Criteria

Other common sources of criteria include OMB Circular A-130, OMB Circular A-123, Presidential Executive Order 14028, and the Federal Risk and Authorization Management Program (FedRAMP).[31]

- OMB Circular A-130 establishes minimum privacy and information security requirements for federal organizations. The appendix to this circular also include responsibilities for protecting federal information resources and managing personally identifiable information.

- OMB Circular A-123 provides guidance to federal organizations on the management of internal controls. It outlines the responsibilities of federal organizations for establishing and maintaining effective internal controls over operations and assets, including requirements for conducting periodic assessments of internal controls and for addressing any identified deficiencies.

- Presidential Executive Order 14028 includes requirements for federal organizations to improve areas such as increasing threat information sharing, modernizing federal government cybersecurity, enhancing software supply chain security, and improving the federal government's detection and handling of threats and vulnerabilities.

- FedRAMP establishes security requirements and guidelines that are intended to help secure cloud computing environments used by agencies and meet the provisions of FISMA and implementing

[29] National Institute of Standards and Technology, *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Gaithersburg, MD: January 2020).

[30] National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, SP 800-161, Revision 1 (Gaithersburg, MD: May 2022).

[31] Office of Management and Budget, *Management's Responsibility for Internal Control*, OMB Circular No. A-123 (Washington, D.C.: December 2004); Office of Management and Budget, *Financial Management Systems*, OMB Circular No. A-127 (Washington, D.C.: October 2009); the White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* Executive Order 13800 (Washington, D.C.: May 11, 2017); and the White House, *Executive Order on Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

guidance.[32] FedRAMP's requirements and guidelines specify the actions agencies and cloud service providers should take in order to authorize cloud services through the program. Further, OMB requires agencies to authorize information systems prior to their operation and periodically thereafter. This requirement also applies to the use of cloud services. Further, FedRAMP uses guidelines based on NIST 800-53 guidelines to provide standardized security requirements for cloud services.

Many other sources may be used to identify more specific technical criteria. The NIST National Checklist Program is a program managed by NIST that provides a repository of cybersecurity-related checklists for use by federal and other organizations.[33] The checklists are developed by federal and non-federal organizations and they provide guidance and recommendations for implementing and maintaining effective cybersecurity controls and practices for areas such as system and network security, access control, and privacy. Furthermore, vendor guidance developed for various types of software can often be accessed by searching the vendor's website. The auditor can also use technical guidance, such as the security technical implementation guides (STIGS) developed by the Defense Information Systems Agency (DISA) as a source of configuration guidance for network devices, software, databases, and operating systems.[34]

Additional applicable criteria includes binding operational directives (BOD) and emergency directives (ED). These directives were developed by CISA to improve the cybersecurity of federal organizations.[35] BODs are issued to address significant cybersecurity threats, vulnerabilities, or risks that require urgent action on the part of federal organizations. EDs are issued in response to urgent or emerging cybersecurity threats that require immediate action to protect federal information systems. Both directives include time-sensitive instructions and requirements for federal organizations to address threats.

For additional criteria and resources, please refer to the criteria section in each chapter. Further, for illustrative examples on how to use these sources of criteria and examples of audit procedures, refer to the supplement to this guide.

Develop Initial Audit Plan

Developing an initial audit plan is an effective and efficient way to obtain the evidence necessary to support the objectives of the audit. A written audit plan must be prepared for any performance audit conducted in accordance with GAO Yellow Book requirements.[36] The nature and extent of audit planning varies for each audit depending on several factors, including the organization's size and complexity, and the audit team's knowledge of the organization's operations.

The form and content of the written audit plan may vary among audits and may include an audit strategy, audit program, project plan, audit planning paper, or other appropriate documentation of the basis for key decisions about the audit objectives, scope, and methodology. Another item to address is to determine which stakeholders are key reviewers or advisors. It may involve consultation with multiple stakeholders, specialists, or subject manner experts. Further, in developing the audit plan, include steps to follow up on the recommendations made in previously issued reports, including findings in prior plans of actions and milestones (POA&M) that are relevant to the audit objectives.

[32] The FedRAMP Authorization Act amends chapter 36 of title 44, United States Code and codifies the FedRAMP program for providing a standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information.

[33] https://ncp.nist.gov/repository/.

[34] https://public.cyber.mil/stigs/.

[35] https://www.cisa.gov/directives/.

[36] GAO, *Government Auditing Standards*, 2018 Revision, GAO-21-368G (Washington, D.C.: April 2021).

The audit plan may include dates for each planned key step and milestone of the audit process. While the specific steps of the audit will vary by organization, the audit team should estimate the amount of time each step will take. Update the plan, as necessary, to reflect any significant changes to the plan made throughout the audit.

Develop Audit Procedures

Documenting audit procedures is a dynamic process that must be considered during design to ensure that sufficient access, evidence, and audit resources are available to fulfill the audit's objectives. Audit procedures are the specific steps and tests auditors perform to address the audit objectives. This guide includes a supplement with illustrative examples of audit procedures. Depending on the audit's objectives, these examples may be beneficial to the audit team in designing its specific procedures.

Consider Risk Factors Significant to Audit Objectives from Internal Controls or Other Factors

A key factor in improving accountability in an organization is to implement an effective internal control system, which helps an organization adapt to shifting environments, evolving demands, changing risks, and new priorities.[37] The audit team should determine if internal controls or other risk factors may be significant to the audit's objectives and document those determinations. The team should reassess this periodically throughout the audit.

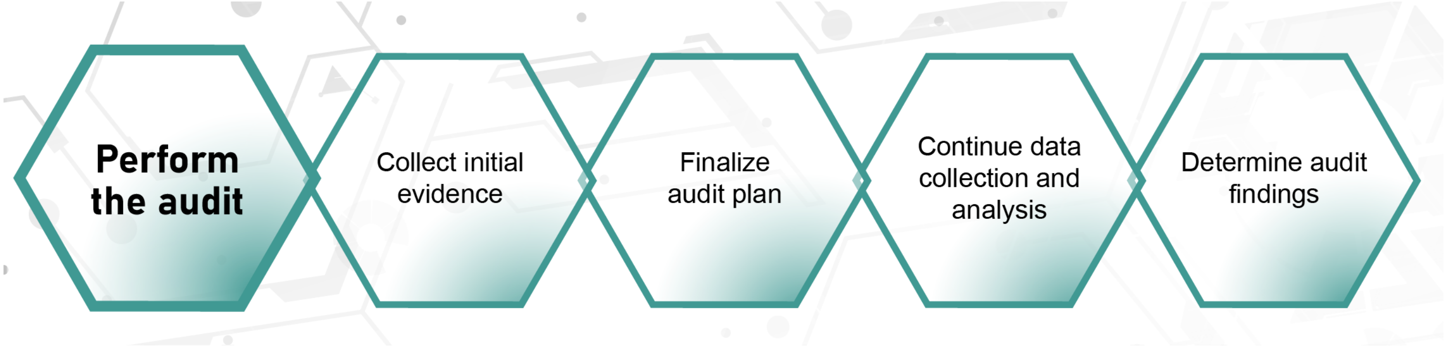
The internal control components to consider with respect to audit objectives include the following:

- **Control environment.** The structure, roles, or responsibilities that the organization's management designs and assigns to personnel and standards of conduct, training, competence, or accountability of personnel.
- **Risk assessment.** The organization's definition of objectives or identification or analysis of risk.
- **Control activities.** The design or implementation of the organization's policies, procedures, actions, or information systems that have been established to achieve its objectives and respond to risk.
- **Information and communication.** The organization's use of information to communicate within the organization or to external parties.
- **Monitoring.** The organization's identification of internal control deficiencies or corrective actions of deficiencies.

In addition to internal controls, the audit team should consider any risks to the audit. These risks could include the nature of the hardware and software, type of processing, extent of peripheral access, highly customized software, limited audit trails, and new technology. If these factors have a significant impact on the audit objectives, implement and document necessary changes to objectives.

[37] According to the GAO Yellow Book, internal control is a process that provides reasonable assurance that the objectives of an organization will be achieved.

1.2 Perform the Audit



Source: GAO. | GAO-23-104705

The key phases of performing the audit are (1) collecting initial evidence, (2) finalizing the audit plan, (3) continuing data collection and analysis, and (4) determining audit findings.

1.2.1 Collect Initial Evidence

Evidence may be categorized as *physical*, *documentary*, or *testimonial*.

Physical evidence is obtained by auditors' direct inspection; walk-through; or observation of people, property, or processes.[38] Such evidence may be recorded in summary memos, photographs, videos, drawings, charts, maps, or physical samples. Prior to obtaining physical evidence, consider whether or not permission will be needed from the organization to do so. For example, auditors may be permitted to take photographs of a publicly accessible building's exterior as part of gathering evidence related to physical security, but may need to obtain permission to take photographs inside of the facility.[39] Other examples may include records of video surveillance and key cards.

Documentary evidence is information that already exists, such as copies of policies and procedures, results of scans previously performed by the organization, screenshots, training records, event and access logs, spreadsheets, database extracts, management information on performance, and other organization-developed documentation.[40] Additional examples of documentary evidence collected during cybersecurity audits include

- inventories of major information systems;
- related audit reports;
- system security plans;
- contingency and disaster recovery plans;
- risk assessments;

[38] A walk-through includes an auditor making observations throughout a facility as guided by audit procedures.

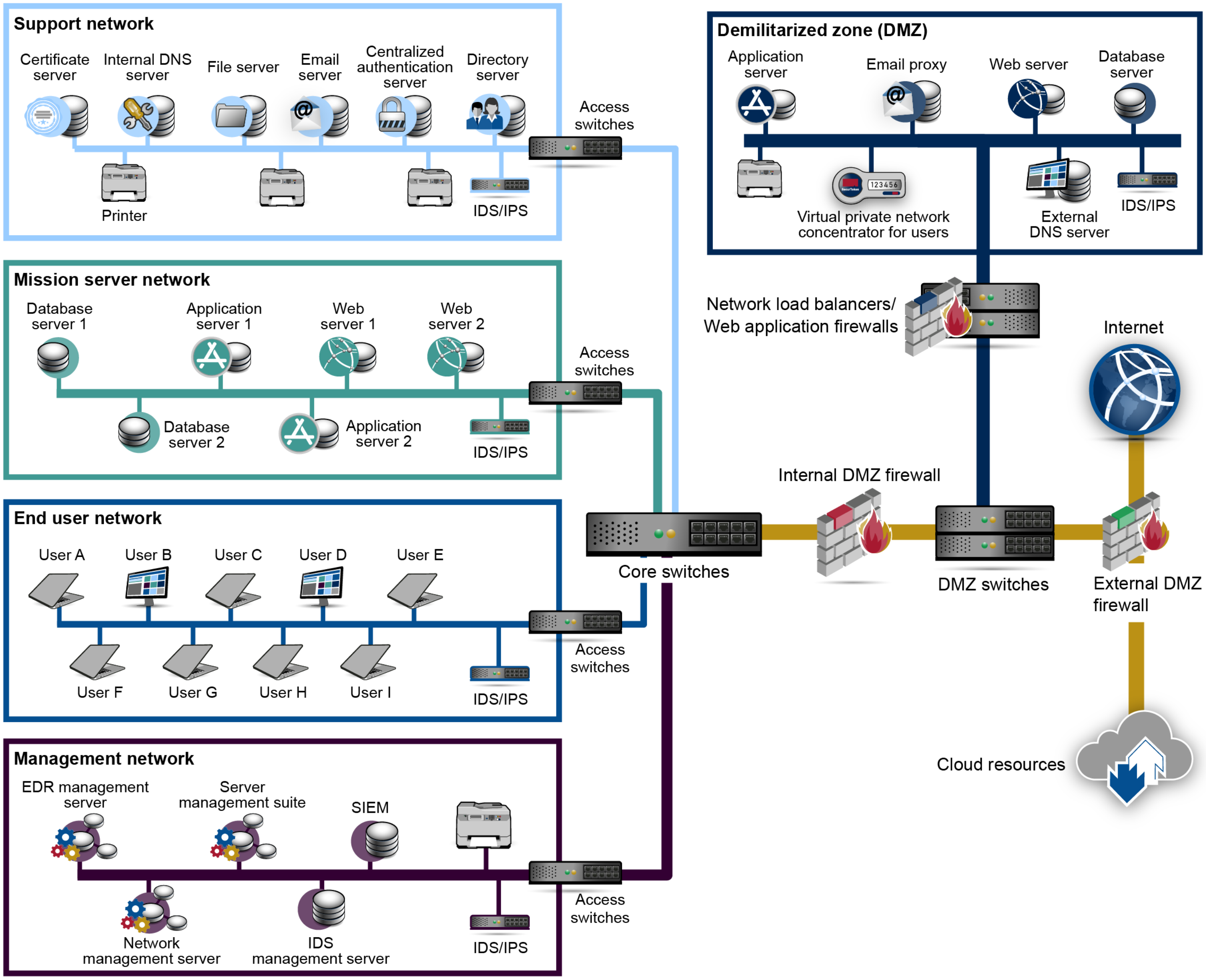
[39] Questions regarding taking photographs may need to be elevated to the auditor's legal counsel.

[40] The specific type of documentary evidence to request will depend on the objectives and scope of the audit as well as the organization's network architecture and specific system(s) being audited, particularly if the organization employs certain cloud services. For example, information security program documentation associated with the cloud services provider and current hardware, software, and firmware inventories for a system that employs a dynamic, rapidly scaling infrastructure as a service solution.

- privacy impact assessments;
- security control assessments;
- security assessment reports;
- corrective action plans, also known as plans of actions and milestones (POA&M);
- concepts of operations;
- network diagrams;
- agreements with external entities;
- lists of tools used for forensic analyses, intrusion detection, and configuration and patch management;
- system authorization packages;
- lists of cybersecurity incidents (within a set time frame);
- vulnerability, patch management, and configuration management scans;
- inventories of select network devices; and
- lists of active security control waivers.

Figure 6 illustrates a network diagram which is an example of documentary evidence that may be collected during the audit.

Figure 6: Example of Documentary Evidence to Collect: A Network Diagram



DNS (domain name server), IDS/IPS (intrusion detection system/intrusion revention system), EDR (endpoint detection and response), SIEM (security information and event management)

Source: GAO (analysis and icons). | GAO-23-104705

Testimonial evidence is obtained through inquiries, interviews, focus groups, public forums, or questionnaires. The evidence gathered should then be evaluated to determine if it is sufficient and appropriate, including ensuring it is relevant, valid, and reliable. Refer to GAO's Yellow Book 8.9-8.107 for more information on the collection and types of evidence that can be collected to develop supporting documentation.

Assess Data Reliability

The reliability of computerized data and of the systems that process, maintain, and report that data is an important consideration in conducting most audits. For cybersecurity audits, the reliability of sources such as logs, databases, and records is critical to their use to support audit findings.
The process for the data reliability assessment includes several key stages and takes into account the expected importance of the data, the strength of corroborating evidence, and the risk of using the data, along with what is learned during the assessment. To assist in assessing data reliability, refer to GAO guidance,

Assessing Data Reliability.[41] The exact procedures needed to assess reliability of computerized data, included any related cybersecurity controls, will vary based on the audit objectives, significance of the data source to the audit findings, and other factors.

1.2.2 Finalize Audit Plan

Before finalizing the audit plan, the audit team should do sufficient initial testing of essential data to provide reasonable assurance of its availability and reliability. Availability is important because if the team cannot access applicable data, or data needed to address objectives does not readily exist, the team will need to reassess its objectives. Reliability is key because if the data are unreliable, the team will not be able to use them to support conclusions and recommendations. In finalizing the plan, the audit team should reflect changes in objectives, scope, audit procedures, time, and resources.

1.2.3 Continue Data Collection and Analysis

Subsequent to finalizing the audit plan, the team should continue data collection and analysis consistent with the plans. In analyzing evidence, particularly for control assessments, a combination of examinations, interviews, and tests may be appropriate.

- *Examinations* include reviewing, inspecting, observing, walk-throughs, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The purpose of examinations is to facilitate the auditor’s understanding, achieve clarification, or obtain evidence.

- *Interviews* include holding discussions with individuals or groups of individuals within an organization to facilitate the auditor’s understanding, achieve clarification, or obtain evidence.

- *Tests* include exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare an actual state to a desired state or expected behavior. Refer to the supplement to this guide and NIST SP 800-53A for more detailed audit steps.

Certain controls lend themselves to one or two methods of assessment while others can be assessed using all three methods. Controls that leave documented evidence of their existence and application (such as logs) may be examined by inspecting such evidence. However, for controls where sufficient evidence cannot be obtained through walk-throughs in combination with observation, inquiry, and other non-sampling tests, obtain evidence by using sampling procedures to select individual items for inspection.[42]

1.2.4 Determine Audit Findings

At this stage, it is particularly important to assess the sufficiency of evidence. When analyzing evidence, the audit team should assess:

- documentation of the nature, timing, and extent of the tests;

- evidence of the effective operation of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools, and related analysis);

[41] GAO, *Assessing Data Reliability*, GAO-20-283G (Washington, D.C.: December 2019).

[42] The network architecture and type of system(s) being audited may impact the type of assessments an auditor can perform, particularly in the case of industrial control systems—systems used to control industrial processes such as manufacturing, product handling, production, and distribution—and cloud services. Review guidance specific to those technologies when determining the appropriate assessment(s) to perform. For example, when reviewing an organization that employs cloud services solution, consult NIST SP 800-144, NIST SP 800-146, and NIST SP 800-190. When reviewing industrial control systems, consult NIST SP 800-82.

- any compensating controls or other factors and the basis for determining effectiveness;
- for each evaluative finding, the criteria, condition, cause, and effect; and
- conclusions and recommendations flowing from the evaluative findings

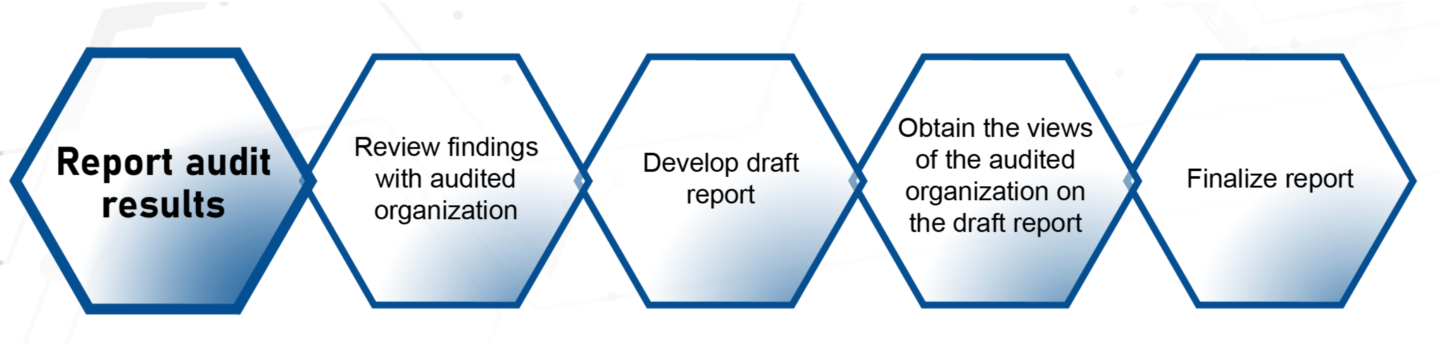
Reviewing the evidence and determining findings should include identifying any gaps in information and following up with the audited organization, as necessary, to request additional evidence or clarification before completing its analyses.

Develop Recommendations

Recommendations may be developed based on the engagement's conclusions. To be most effective, recommendations should

- clearly identify the proposed action to be taken;
- logically arise from the evidence presented;
- clearly link to the objectives and findings;
- specify actions that are feasible, cost-effective, and measurable;
- be well-supported and convincing;
- address the cause of identified deficiencies; and
- be addressed to the organization's official with the responsibility and authority to act on them.

1.3 Report Audit Results


Report audit results
Review findings with audited organization
Develop draft report
Obtain the views of the audited organization on the draft report
Finalize report

Source: GAO. | GAO-23-104705

After performing the audit work, (1) review the findings with the audited organization, (2) develop a draft report, (3) obtain the views of the audited organization on the draft report, and (4) finalize the report.

1.3.1 Review Findings with Audited Organization

Upon completion of the audit work, the audit team should provide the audited organization a statement of facts that describes the audit findings. The organization can comment on and discuss the statement of facts with the auditors, and provide feedback and supporting documentation that may impact the findings and recommendations. During this time, discuss any sensitivity issues the organization may have and update the draft report accordingly. Any findings that warrant immediate remediation should be communicated to the organization throughout the audit, as appropriate.

1.3.2 Develop Draft Report

Audit reports should present audit results in a clear and understandable format. The report should include the audit objectives, scope, methodology, findings, conclusions, and recommendations. Information provided by the audited organization based on the statement of facts should be incorporated as appropriate in the report. Furthermore, the use of graphics and tables is encouraged to enhance the readability and clarity of the report.

1.3.3 Obtain Views of the Audited Organization on the Draft Report

Providing a draft report with findings for review and comment by responsible officials of the audited organization helps develop a report that is fair, complete, and objective. Written comments from an organization are preferred, but oral comments are acceptable.

Determine Sensitivity of Reports

In reporting on cybersecurity audits, organizations often develop two reports—a public report and a sensitive version containing content that cannot be released to the public. A key advantage of a sensitive report is the additional detail it can provide on the organization and audit findings. However, a disadvantage is the risk of disclosure, particularly in cases where the report is issued to an organization that shares it with a large number of staff to facilitate remediation. A public report has a broader audience and greater transparency but cannot contain sensitive information.

To avoid public disclosure of sensitive information, provide draft cybersecurity reports to the organization for a sensitivity review. Upon receiving the results of the sensitivity review, make appropriate report revisions.

Depending on the audit, a public report, a sensitive report, or both could be issued. Cybersecurity audit reports for federal organizations may or may not be put on the organization's websites or released under the Freedom of Information Act.[43] Reports not posted on the organization's websites or otherwise made available to the public are still typically issued to organization management and others on a need to know basis.

Non-federal organizations may be subject to additional state laws and regulations that affect the form of reporting. When the audit organization is subject to public records laws, such as the Freedom of Information Act or other similar state-specific legislation, determine whether public records laws could affect the availability of sensitive reports.[44]

1.3.4 Finalize Report

After the audited organization has had sufficient time to review and comment on the draft report, the audit team can then finalize the audit report. Finalizing the audit report includes addressing comments made in the audited organization's comment or signed management response letter. If oral comments are provided instead, identify in the audit report the source within the organization of those comments. Upon completion of these steps, the audit team can proceed with its organization's publication and distribution process.

[43] The Freedom of Information Act (FOIA) generally provides that any person has the right to obtain access to federal agency records except to the extent those records are protected from disclosure by the FOIA. Federal agencies are generally required to disclose any information requested under the act unless it falls under one of nine enumerated exemptions.

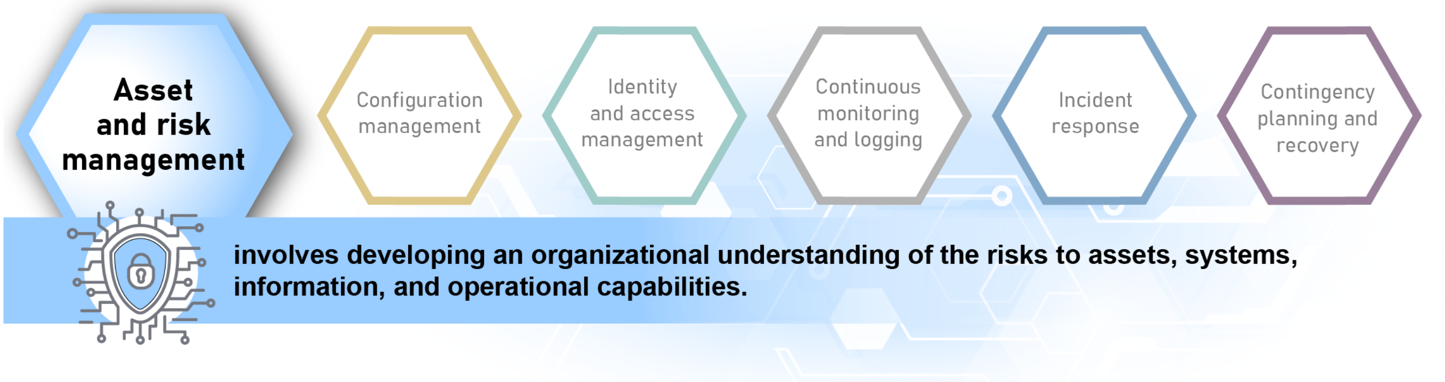
[44] When the auditor identifies or suspects noncompliance with provisions of laws, regulations, contracts, or grant agreements or instances of fraud, the auditor may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. The auditor may limit public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record.

Asset and risk management

2

Source: GAO; images: Looker_Studio/stock.adobe.com, marinashevchenko/stock.adobe.com and ixtumz88/stock.adobe.com. | GAO-23-104705

Chapter 2. Asset and Risk Management Audit Steps


Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery

involves developing an organizational understanding of the risks to assets, systems, information, and operational capabilities.

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

2. Asset and Risk Management

Key Practices in This Chapter

2.1 Assess IT governance: determine the extent to which the organization has effective and efficient use of IT to enable it to achieve its goals and mission.

2.2 Assess management of assets: determine the extent to which the organization manages what is on its network, including all authorized hardware and software, and virtual systems.

2.3 Assess risk management strategy: determine the extent to which the organization assesses risk, responds to risk, and monitors risks associated with the use and operation of its information systems.

2.4 Review risk assessment: determine the extent to which the organization identifies and considers all threats and vulnerabilities, identifies the greatest risks, and makes appropriate decisions regarding which risks to accept and which to mitigate through security controls.

2.5 Review plans of actions and milestones: determine the extent to which that the organization can effectively document planned remedial actions to correct deficiencies and reduce or eliminate known vulnerabilities in the system.

2.6 Assess management of supply chain risk: determine the extent to which the organization identifies the range of risks from contractors and other users across the supply chain with privileged access to its systems, applications, and data.

2.7 Evaluate security awareness and training program: determine the extent to which that the organization establishes and implements effective training policies.

Note: The use of "should" statements within key practices does not indicate a requirement unless explicitly stated in criteria. Auditors using this guide should apply professional judgment when determining which key practices and audit steps to implement.

Examples of Criteria to Consider

In addition to the criteria discussed in the "Identify Criteria" section of this guide, consider the following examples of criteria to use:

NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, SP 800-161, Revision 1 (Gaithersburg, MD: May 2022): provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain.

NIST, *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e* (Gaithersburg, MD: February 2022): provides guidance in accordance with the executive order that provides recommendations to federal organizations on ensuring that producers of software they procure have been following a risk-based approach for secure software development throughout the software lifecycle.

NIST, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities,* SP 800-218 (Gaithersburg, MD: February 2022): provides a core set of high-level secure software development practices that can be integrated into software development implementation to reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.

NIST, *Guide for Conducting Risk Assessments,* SP 800-30 Revision 1 (Gaithersburg, MD: September 2012)*:* provides guidance for conducting risk assessments of federal information systems and organizations.

NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, MD: March 2011): provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems.

NIST, *Standards for Security Categorization of Federal Information and Information Systems Federal Information Processing Standards (FIPS) 199* (Gaithersburg, MD: February 2004): provides a standard for categorizing federal information and information systems according to (1) an agency's level of concern for confidentiality, integrity, and availability; and (2) the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.

NIST, *Building an Information Technology Security Awareness and Training Program,* SP 800-50 (Gaithersburg, MD: October 2003): provides guidance for building an effective IT security program and supports requirements specified in the Federal Information Security Management Act (FISMA) of 2002.

NIST, *Information Technology Security Training Requirements: A Role and Performance-Based Model,* SP 800-16 (Gaithersburg, MD: April 1998): provides a framework for IT security training.

Department of Homeland Security (DHS), *Securing High Value Assets,* BOD 18-02 (May 7, 2018): contains requirements for federal organizations to take specific actions to protect their most critical systems.

OMB, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, M-22-18 (Washington, D.C.: Sept. 14, 2022): requires each federal agency to comply with the NIST guidance when using third-party software on the agency's information systems or otherwise affecting the agency's information.

2.1 Assess IT Governance

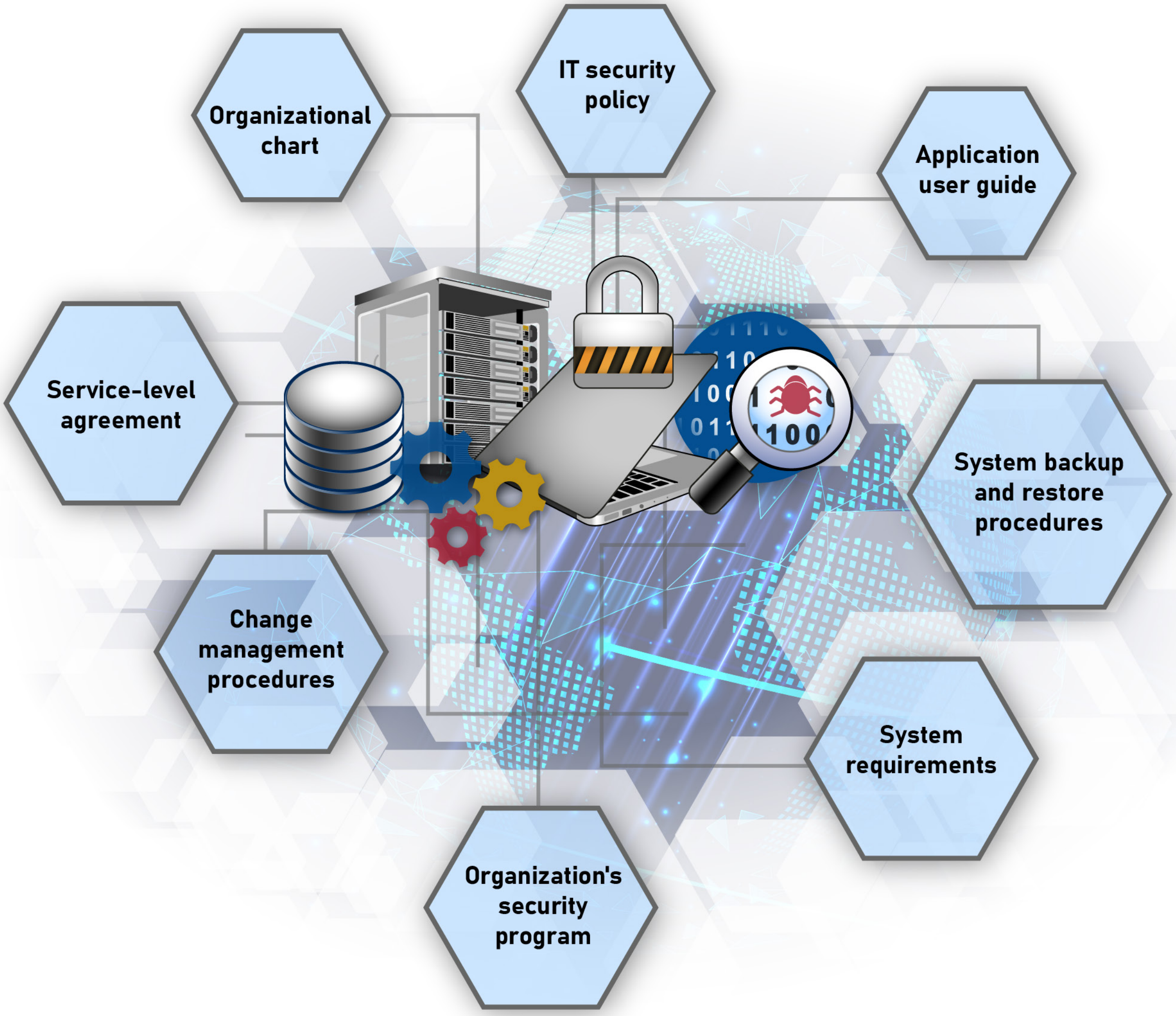
IT governance is defined as the processes that ensure the effective and efficient use of IT to enable an organization to achieve its goals and mission. Effective IT governance fosters and maintains a focus on key decisions that may have an impact on business performance. IT governance can include numerous areas such as leadership, organizational structures, and processes that sustain and extend an organization's IT strategies and objectives. However, governance related to cybersecurity is typically of most importance to a cybersecurity audit. According to NIST, IT governance documentation includes organizational requirements, policies, procedures, plans, programs, organizational charts, and processes to manage and monitor cybersecurity risks.[45]

Organizational cybersecurity policy is central to IT governance, and it is essential that the policy be established and communicated throughout the organization. According to FISMA, each federal organization information security program must include policies and procedures that are based on risk assessments that cost effectively reduce information security risks to an acceptable level. Security policy is senior management's directive to create an IT security program, establish its goals, and assign responsibilities. The term is also used to refer to specific security rules for particular systems. Because security policy is written at a broad level, organizations also develop standards, guidelines, and procedures that offer users, managers, and others a clear approach to implementing security policy and meeting organizational goals.

Figure 7 provides an example of the types of documentation an auditor may consider, request, and review to determine if an organization has established policies, processes, and procedures related to cybersecurity and maintaining the confidentiality, integrity, and availability of its IT assets.

[45] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: April 2018).

Figure 7: Examples of an Organization’s IT-Related Documentation



Source: GAO; images: GAO and SergeyBitos/stock.adobe.com. | GAO-23-104705

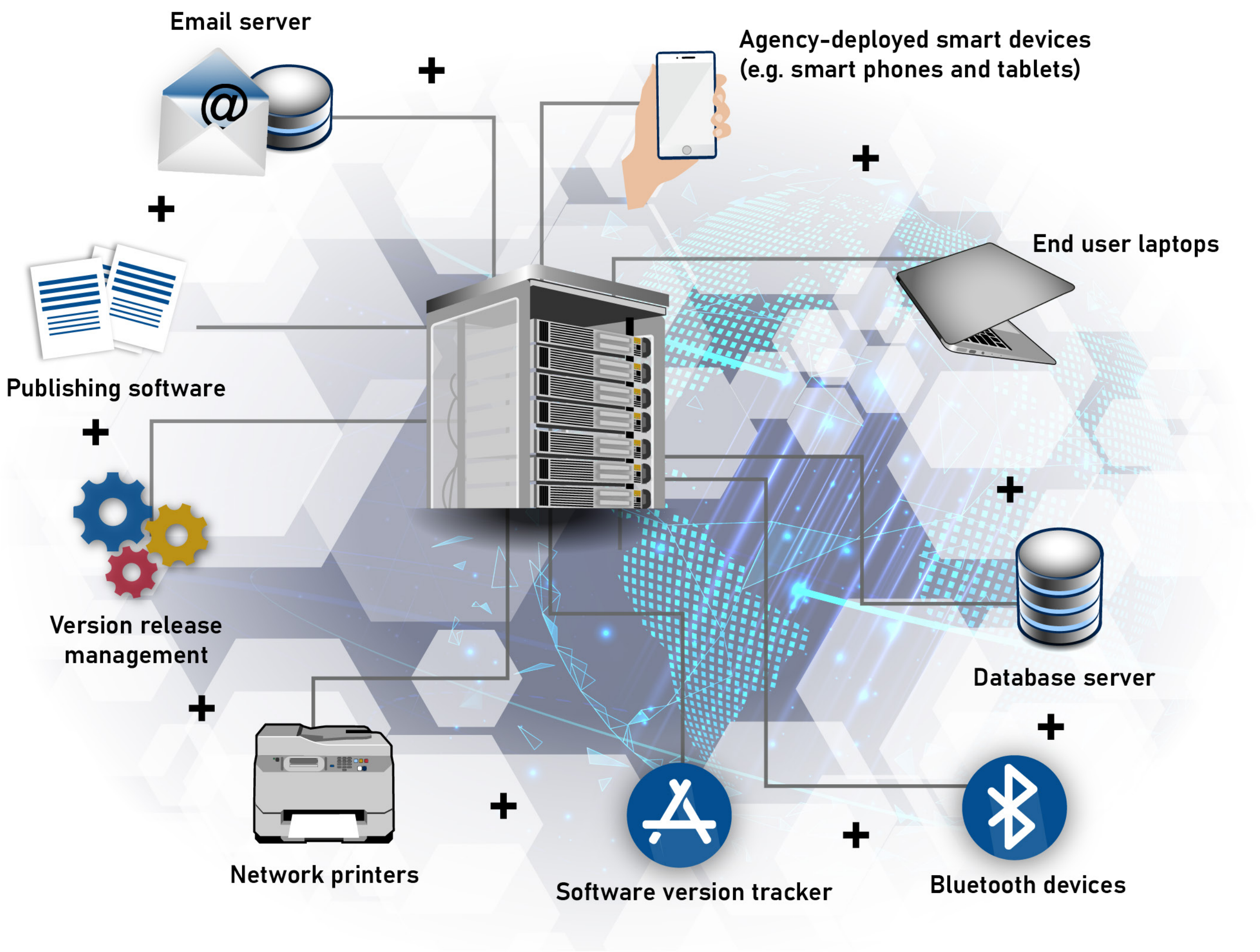
Control Objectives and Audit Procedures

Key practice 2.1 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization’s IT governance. These are a sample of controls and not the only controls that could be considered. Professional judgment should be used to determine which controls are appropriate for the audited organization. Additionally, these audit procedures should be considered for systems under the control of the organization. For example, these procedures may not apply to systems owned or managed by a contractor or other third-party.

2.2 Assess Management of Assets

According to NIST, management of assets involves managing what is on an organization's network to effectively manage, use, and secure each of those assets.[46] Figure 8 provides a sample of the types of items on an organization's network that an auditor may consider when reviewing the controls for asset management.

Figure 8: Sample of Identified Items on an Organization's Network



Source: GAO; images: GAO and SergeyBitos/stock.adobe.com. | GAO-23-104705

Asset management can help organizations optimize funding and decision-making to better target their policy goals and objectives. Effective asset management can also help to foster a culture of effective decision-making through leadership support, policy development, and staff training. Asset management policies and procedures should address purpose, scope, roles, responsibilities, compliance, and implementation of asset management security controls.

[46] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: April 2018).

Control Objectives and Audit Procedures

Key practice 2.2 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization’s management of assets.

2.3 Assess Risk Management Strategy

A risk management strategy addresses how organizations intend to assess risk, respond to risk, and monitor risk associated with the use and operation of information systems. According to NIST, agencies should develop a cybersecurity risk management strategy to provide a foundation for managing risk and delineate the boundaries for risk-based decisions.[47] The strategy should describe the strategic-level decisions and considerations that senior leaders and executives are to use to manage security and privacy risks to the organization’s operations and assets, among others. The strategy should also guide and inform how security and privacy risks are framed, assessed, responded to, and monitored. The strategy should include (1) a statement of the organization’s risk tolerance, (2) how the organization intends to assess risk (e.g., acceptable risk assessment methodologies), (3) acceptable risk response strategies (e.g., acceptance, mitigation, and avoidance), and (4) how the organization intends to monitor risk over time.[48]

Control Objectives and Audit Procedures

Key practice 2.3 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization’s risk management strategy.

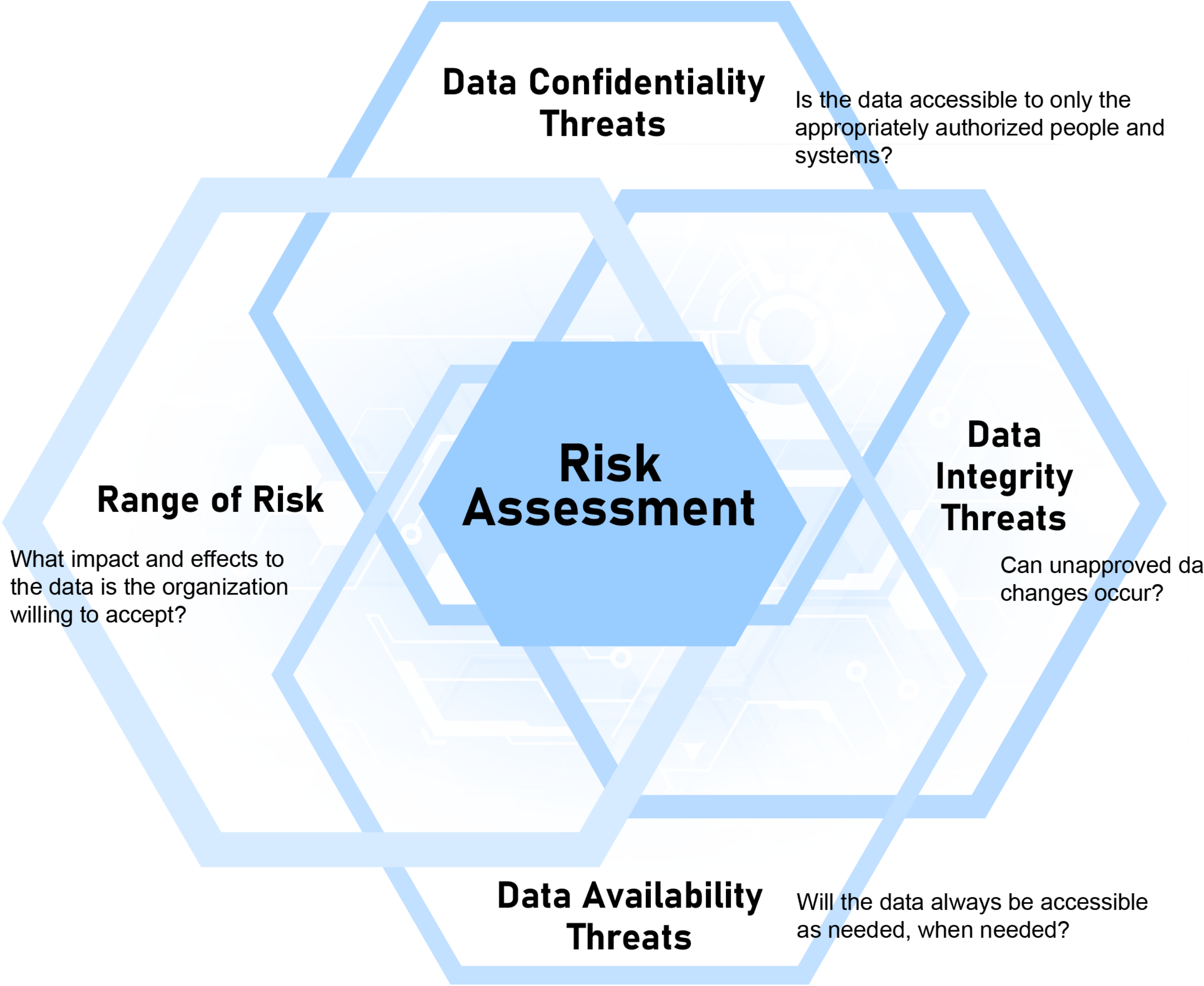
2.4 Review Risk Assessment

According to NIST, a risk assessment is the process of identifying risks to organizational operations, organizational assets, individuals, other organizations, and the nation resulting from the operation of an information system. A comprehensive risk assessment should be the starting point for developing or modifying an organization’s security policies and security plans. NIST states that a risk assessment is one of the fundamental components of an organization’s risk management. Such assessments are important because they help make certain that all threats and vulnerabilities are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls. Figure 9 contains examples of risk assessment questions auditors may consider.

[47] National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, MD: March 2011).

[48] According to NIST, risk tolerance is the degree of risk or uncertainty that is acceptable to an organization.

Figure 9: Example of Risk Assessment Questions Auditors May Consider


Data Confidentiality Threats
Is the data accessible to only the appropriately authorized people and systems?
Range of Risk
What impact and effects to the data is the organization willing to accept?
Risk Assessment
Data Integrity Threats
Can unapproved data changes occur?
Data Availability Threats
Will the data always be accessible as needed, when needed?

Source: GAO; images: pixtumz88/stock.adobe.com.. | GAO-23-104705

Risk assessments should consider threats to data confidentiality, integrity, and availability, and the range of risks that an organization's systems and data may be subject to, including those posed by both authorized and unauthorized users. For example, risk assessments should take into account observed trends in the types and frequency of hacker activity and threats. Such analyses should also draw on reviews of system and network configurations, as well as observations and testing of existing security controls.

Risk assessment controls help ensure

- critical IT assets are identified and included in the risk assessment,
- asset vulnerabilities are identified and documented,
- cyber threat intelligence is received from information sharing forums and sources,
- threats, both internal and external, are identified and documented,
- potential business impacts and likelihoods are identified,
- threats, vulnerabilities, likelihoods, and impacts are used to determine risk, and
- risk responses are identified and prioritized.

Control Objectives and Audit Procedures

Key practice 2.4 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's risk assessment.

2.5 Review Plans of Actions and Milestones

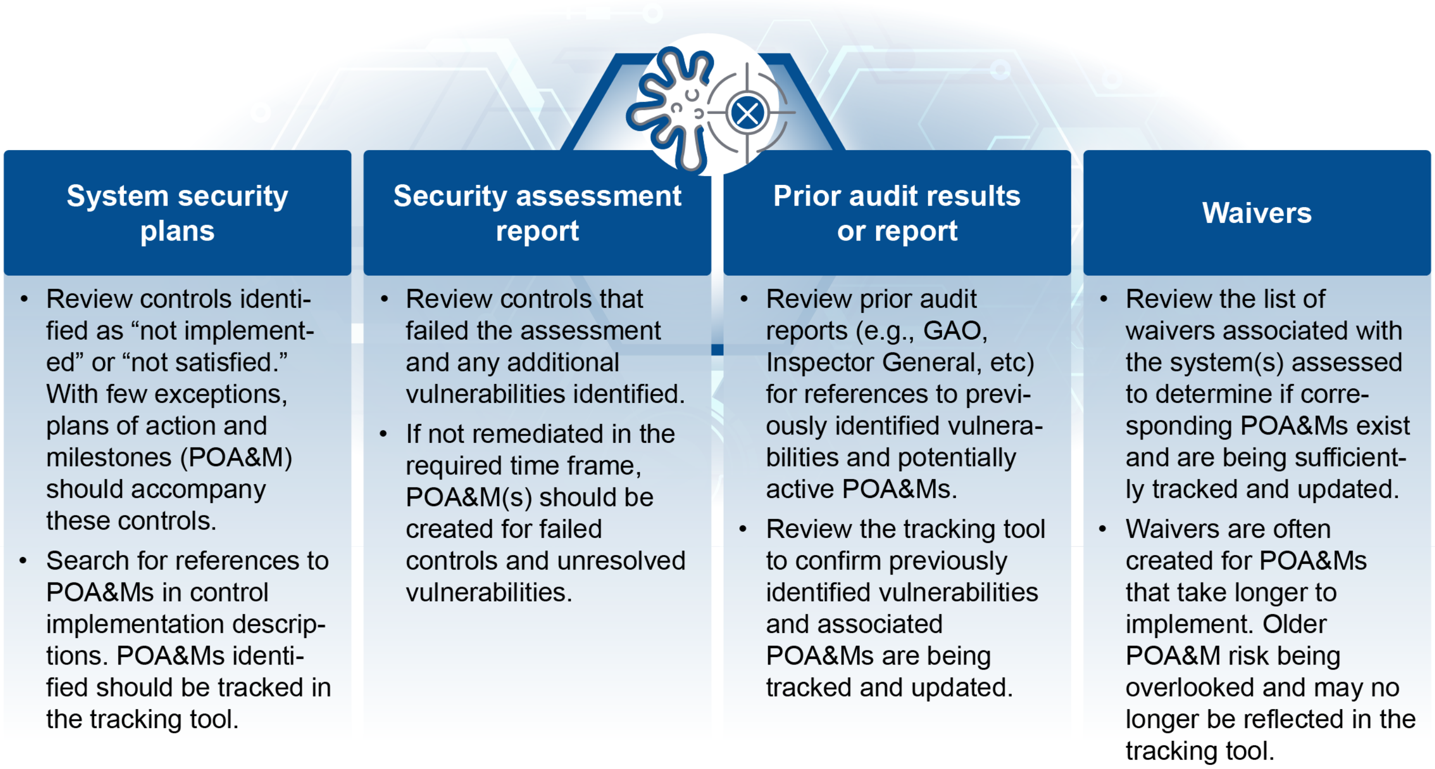
According to NIST, POA&Ms are corrective action plans that document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.[49] The POA&M process is an important element of an organization's risk management capability because it is a mechanism for tracking and remediating identified incidents. Further, organizations should update existing POA&Ms based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. Additionally, FISMA requires that organization-wide information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization.[50]

When considering appropriate corrective actions to be taken, the organization should, to the extent possible, consider the potential organization-wide implications and design appropriate corrective actions to systemically address the deficiency. See figure 10 for examples of when organizations should develop POA&Ms and suggestions as to how auditors can assess whether they have been developed and tracked appropriately.

[49] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[50] 44 USC §3554(b)(6).

Figure 10: Documents to Review When Assessing Plans of Action and Milestones



System security plans

- Review controls identified as "not implemented" or "not satisfied." With few exceptions, plans of action and milestones (POA&M) should accompany these controls.
- Search for references to POA&Ms in control implementation descriptions. POA&Ms identified should be tracked in the tracking tool.

Security assessment report

- Review controls that failed the assessment and any additional vulnerabilities identified.
- If not remediated in the required time frame, POA&M(s) should be created for failed controls and unresolved vulnerabilities.

Prior audit results or report

- Review prior audit reports (e.g., GAO, Inspector General, etc) for references to previously identified vulnerabilities and potentially active POA&Ms.
- Review the tracking tool to confirm previously identified vulnerabilities and associated POA&Ms are being tracked and updated.

Waivers

- Review the list of waivers associated with the system(s) assessed to determine if corresponding POA&Ms exist and are being sufficiently tracked and updated.
- Waivers are often created for POA&Ms that take longer to implement. Older POA&M risk being overlooked and may no longer be reflected in the tracking tool.

Source: GAO analysis based on National Institute of Standards and Technology publications; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

- In addition, NIST defines the minimum information organizations should include when developing POA&Ms.[51] Furthermore, NIST states that the organization should track POA&Ms in an organization-wide tracking tool in order to facilitate both implementation and oversight. See figure 11 for examples of information organizations should include when developing POA&Ms.

[51] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

Figure 11: Assessing Elements of a Plan of Actions and Milestones (POA&M)

Associated vulnerability	Assess whether the POA&M identifies the vulnerability prompting its creation.
Responsible individual or office	Assess whether the POA&M identifies the individual or office that the organization head will hold responsible for resolving the vulnerability.
Resources required	Assess whether the POA&M identifies the resources required, such as funding or personnel hours, to implement the remedial action and, if required, organizational guidance.
Originally scheduled completion date	Assess whether the POA&M identifies the originally scheduled completion date.
Currently scheduled completion date	Assess whether the POA&M identifies the currently scheduled completion date and that the date is not past due (i.e., predates the last POA&M update).
Milestones, changes, and scheduled completion dates	Assess whether the milestones have been developed and described in the POA&M, to include changes to the milestones and, in the case of completed milestones, actual completion dates.
Completion status	Assess whether the organization identifies the completion of individual POA&Ms as either "ongoing," or "delayed," or "completed" (if complete, check for the completion date).

Source: GAO analysis based on National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

Additional steps can be taken to assess the elements of a POA&M. For example, the following can be verified:

- *Associated vulnerability* - Ensure the description or ID is sufficient to trace the vulnerability to its source. If an ID is listed, consider verifying its accuracy by tracing it to the source (e.g., security assessment report).

- *Originally scheduled completion date* - Review older versions of the POA&M to confirm the originally scheduled completion date has not been updated and does in fact reflect the date at the time the POA&M was developed.

- *Currently scheduled completion date* - Confirm the currently scheduled completion date does not predate the last POA&M update. In addition, review the milestone completion dates to ensure the currently scheduled completion date is on or after the scheduled completion date of the final milestone.

- *Milestones, changes, and scheduled completion dates* - Review previous versions of the POA&M to assess if changes were made to a milestone's scheduled completion date and whether the reason for any change is sufficiently documented.

- *Completion status* - Confirm POA&Ms identified as "delayed" include a description of why they are delayed, any mitigating action(s) taken, and any waivers in place. If completed, assess whether the corrective actions addresses the weakness.

Control Objectives and Audit Procedures

Key practice 2.5 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's POA&Ms.

2.6 Assess Management of Supply Chain Risk

According to NIST, cybersecurity risk throughout the supply chain refers to the potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services.[52] Cybersecurity risks throughout the supply chain are the result of threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself. According to NIST, contractors are considered participants in the supply chain.[53] Government and other private organizations face a range of risks from contractors and other users across the supply chain with privileged access to their systems, applications, and data. Contractors that provide systems and services for other users with privileged access can introduce risks to their information and systems. FISMA information security requirements apply not only to information systems used or operated by an agency but also to information systems used or operated by a contractor of an agency or other agency on behalf of an agency. In addition, the *Federal Acquisition Regulation* requires that federal agencies prescribe procedures for ensuring that federal IT acquisitions comply with the IT security requirements of FISMA; OMB's implementing policies, including OMB Circular A-130; and guidance and standards from NIST.[54]

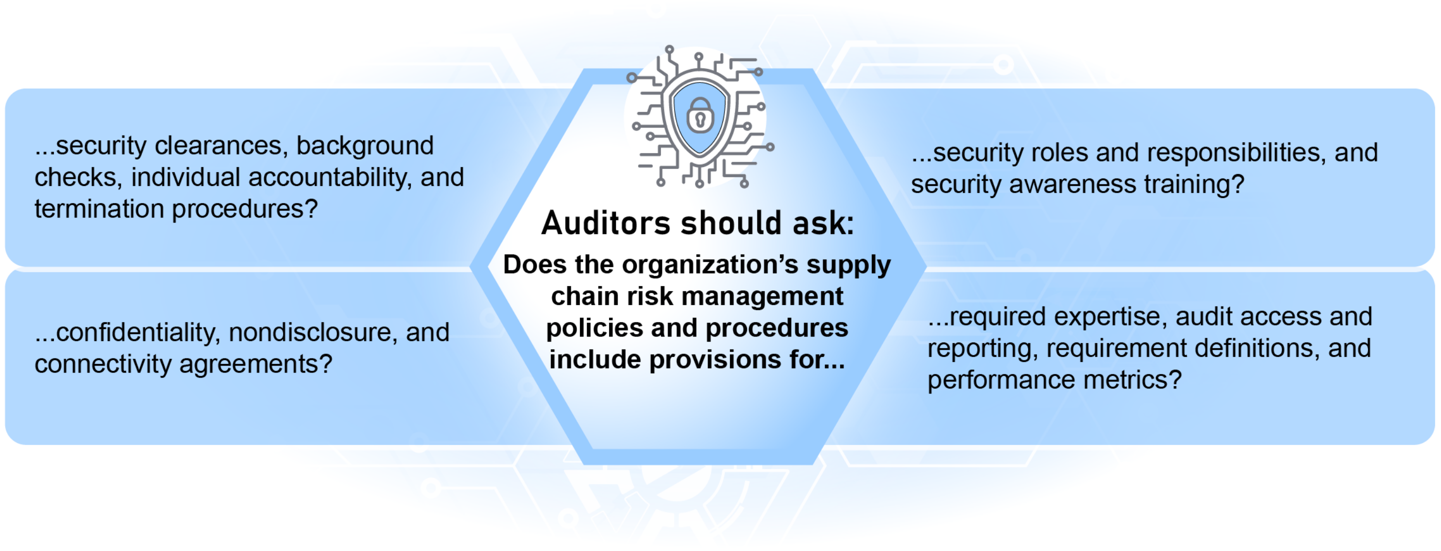
The organization should develop, implement, and monitor policies and procedures to ensure that the activities performed by their external third parties (e.g., service bureaus, contractors, and other service providers of system development, network management, and security management) are documented, agreed to, implemented, and monitored for compliance. These should include provisions for (1) security clearances (where appropriate and required), (2) background checks, (3) required expertise, (4) confidentiality/nondisclosure agreements, (5) security roles and responsibilities, (6) connectivity agreements, (7) individual accountability, (8) audit access and reporting, (9) termination procedures, (10) security awareness training, (11) requirements definition, and (12) performance metrics. In addition, verification should be performed to periodically ensure that the procedures are being correctly applied and consistently followed, including the security of relevant contractor systems. Appropriate controls also need to be applied to outsourced software development. Figure 12 contains examples of supply chain risk management questions auditors may consider.

[52] National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,* SP 800-161, Revision 1 (Gaithersburg, MD: May 2022).

[53] National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,* SP 800-161, Revision 1 (Gaithersburg, MD: May 2022).

[54] 48 CFR 7.103(w). *The Federal Acquisition Regulation* was established to codify uniform policies for acquisition of supplies and services by all executive agencies. 48 CFR 1.101.

Figure 12: Example of Supply Chain Risk Management Questions Auditors May Consider


Auditors should ask:
Does the organization's supply chain risk management policies and procedures include provisions for...
...security clearances, background checks, individual accountability, and termination procedures?
...security roles and responsibilities, and security awareness training?
...confidentiality, nondisclosure, and connectivity agreements?
...required expertise, audit access and reporting, requirement definitions, and performance metrics?

Source: GAO; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

Control Objectives and Audit Procedures

Key practice 2.6 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's management of supply chain risk.

2.7 Evaluate the Security Awareness and Training Program

According to NIST, a robust and enterprise-wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and proper use and protection of the IT resources entrusted to them.[55] An ongoing security awareness and training program should be implemented that includes first-time training for all new employees, contractors, and users, and annual training for all employees, contractors, and users. According to FISMA, an agency-wide information security program for a federal agency must include security awareness training for not only the organization's personnel but also contractors and other users of information systems that support the agency's operations and assets.[56] This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with organizational policies and procedures designed to reduce these risks.[57] Additionally, OMB requires personnel to be trained before they are granted access to systems or applications. The training is to make sure that personnel are aware of the system or application's rules, their responsibilities, and their expected behavior.

In addition, employees with significant security responsibilities should receive specialized training. In accordance with 5 CFR 930.301, each executive agency must identify employees with significant information security responsibilities and provide role-specific training in accordance with NIST standards and guidance.

[55] National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program,* SP 800-50 (Gaithersburg, MD: October 2003).

[56] 44 USC §3554(b)(4).

[57] 44 U.S.C. §3554(b)(4)(A) and (B).

FISMA also includes requirements for training personnel with significant responsibilities for information security.[58]

Control Objectives and Audit Procedures

Key practice 2.7 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization’s security awareness and training program.

2.7.1 Assess Training and Expertise Requirements for Employees

The organization’s management should ensure that employees—including data owners, system users, data processing personnel, and security management personnel—have the expertise to carry out their information security responsibilities. To accomplish this, a security training program should be developed that includes areas such as:

- job descriptions that include the education, experience, and expertise required;
- periodic reassessment of the adequacy of employees’ skills; and
- annual training requirements and professional development programs to help ensure that employees’ skills, especially technical skills, are adequate and current.

Control Objectives and Audit Procedures

Key practice 2.7.1 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization’s training and expertise requirements for employees.

2.7.2 Determine Users’ Awareness of Security Policies

For a security program to be effective, those expected to comply with it must be aware of it. Employee awareness is critical in combating security threats posed by spam, spyware, and phishing. In addition, security awareness is considered important in reducing the risk of social engineering where users are talked into revealing sensitive information to potential thieves. Educating users about such risks makes them think twice before revealing sensitive data and makes them more likely to notice and report suspicious activity.

Security awareness should be established and maintained by the organization to include:

- informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality;
- distributing documentation describing security policies, procedures, and users’ responsibilities, including their expected behavior;
- requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for security (including the consequences of security violations) and their responsibilities for following all organizational policies (including maintaining confidentiality of passwords and physical security over their assigned areas); and
- requiring comprehensive security orientation, training, and periodic refresher programs to communicate security guidelines to both new and existing employees and contractors.

[58] 44 U.S.C. §3554(a)(3)(D).

Control Objectives and Audit Procedures

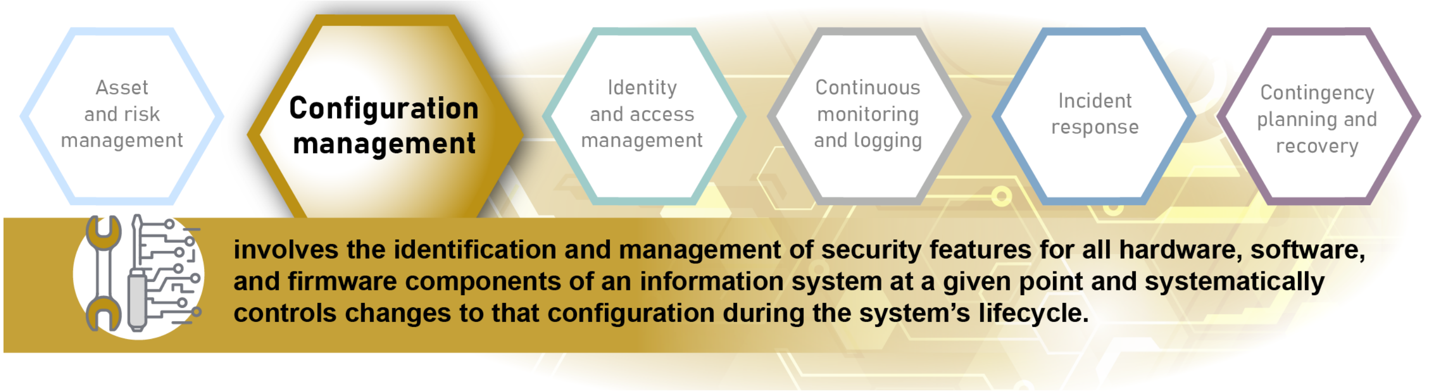
Key practice 2.7.2 in the Chapter 2 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's users' awareness of security policies.

Configuration management

3

Source: GAO; images: ipopba/stock.adobe.com, marinashevchenko/stock.adobe.com and ixtumz88/stock.adobe.com. | GAO-23-104705

Chapter 3. Configuration Management Audit Steps


Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery

involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's lifecycle.

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com and pixtumz88/stock.adobe.com. | GAO-23-104705

3. Configuration Management

Key Practices in This Chapter

3.1 Review configuration management policies, plans, and procedures: determine the extent to which the organization has an established configuration management process.

3.2 Review current configuration identification information: determine the extent to which the organization can identify physical and functional characteristics of a configuration item.

3.3 Assess management of configuration changes: determine the extent to which the organization properly controls all configuration changes.

3.4 Assess configuration monitoring activities: determine the extent to which the organization's current configuration information is routinely monitored for accuracy.

3.5 Assess software update process: determine if the organization has an effective process to scan and update software frequently to guard against vulnerabilities.

3.6 Review documentation on emergency configuration changes: determine the extent to which the organization's emergency changes are documented and approved by the appropriate officials.

Note: The use of "should" statements within key practices does not indicate a requirement unless explicitly stated in criteria. Auditors using this guide should apply professional judgment when determining which key practices and audit steps to implement.

Examples of Criteria to Consider

In addition to the criteria discussed in the "Identify Criteria" section of this guide, consider the following:

NIST, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, SP 800-40, Revision 4 (Gaithersburg, MD: April 2022): includes guidelines to help organizations improve their enterprise patch management planning so that they can strengthen their management of risk.

NIST, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers,* SP 800-70, Revision 4 (Gaithersburg, MD: February 2018)*:* explains how to use the National Checklist Program checklists and describes the policies, procedures, and general requirements for participation in the program.

NIST, *Guide for Security-Focused Configuration Management of Information Systems*, SP 800-128 (Washington, D.C.: August 2011): provides guidelines for organizations responsible for managing and administering the security of federal information systems and associated environments of operation.

NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Washington, D.C.: March 2006): specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements.

DHS, *Improving Asset Visibility and Vulnerability Detection on Federal Networks,* BOD 23-01 (Oct. 3, 2022): contains requirements and implementation guidance on asset discovery and vulnerability enumeration which are essential for improving operational visibility for a successful cybersecurity program.

DHS, *Vulnerability Remediation Requirements for Internet-Accessible Systems,* BOD 19-02 (Apr. 19, 2019): establishes requirements for federal organizations to review and remediate critical vulnerabilities on internet-facing systems.

OMB, *Memorandum for Heads of Executive Departments and Agencies: Completing the Transition to Internet Protocol Version 6* (IPv6), M-21-07 (Washington, D.C.: November 2020): provides guidance on the federal government's operational deployment and use of IPv6 and includes specific steps federal organizations are expected to take to complete the transition.

DISA STIGS: provides an additional source of configuration guidance for network devices, software, databases and operating systems.[59]

[59] https://public.cyber.mil/stigs/.

3.1 Review Configuration Management Policies, Plans, and Procedures

Effective configuration management policies and procedures establish an initial baseline of hardware, software, and firmware components for the organization.[60] According to NIST, configuration management policies and procedures are essential to ensuring adequate consideration of the potential security impact of specific changes to an information system.[61] Configuration management policies and procedures should include employee roles and responsibilities, configuration management and system documentation requirements, establishment of a decision-making structure, and training requirements. These policies and procedures should also address security controls which include (1) a baseline configuration of the information system and an inventory of the system's constituent components, (2) a process to control and monitor changes to the system, (3) a way to assess restrictions over changes to the system and auditing of the enforcement actions, and (4) a method to configure the security settings of IT products to the most restrictive mode consistent with operational requirements. Configuration management documents should be developed, documented, and implemented at the organization, system, and application levels.

The configuration management plan should describe the allocation of responsibilities and authorities for management activities to entities and individuals within the project structure. The management activities implementing configuration management can include use of a configuration control board.

The organization's software development life cycle should include a reference to configuration management. Policies should also address the introduction of software developed outside of the organization's normal software development process, including the outsourced development of software and commercial or other software acquired by individual users.

Control Objectives and Audit Procedures

Key practice 3.1 in the Chapter 3 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's configuration management policies, plans, and procedures. These are a sample of controls and not the only controls that should be considered. Professional judgment should be used to determine which controls are appropriate for the audited organization. Additionally, these audit procedures should be considered for systems under the control of the organization. For example, these procedures may not apply to systems owned or managed by a contractor or other third-party.

3.2 Review Current Configuration Identification Information

Configuration identification activities involve identifying, naming, and describing the physical and functional characteristics of a configuration item (e.g., specifications, design, internet protocol (IP) address, code, data element, architectural artifacts, and documents). FISMA requires federal agency compliance with system configuration requirements, as determined by the organization. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information. The configuration plan should describe how each configuration item and its versions are uniquely named. It should also describe the activities performed to define, track, store, manage, and retrieve configuration items. According to NIST, an organization should also have information system diagrams and documentation on the setup of routers, switches, firewalls, wireless networks, Bluetooth, and any other devices facilitating connections to other systems.[62]

[60] Firmware is a specific class of computer software that provides the low-level control for a device's specific hardware.

[61] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[62] According to CISA, many electronic devices are now incorporating Bluetooth technology to allow wireless communication with other Bluetooth devices. Before using Bluetooth, it is important to understand what it is, what security risks it presents, and how to protect against attacks.

Control Objectives and Audit Procedures

Key practice 3.2 in the Chapter 3 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's current configuration management identification information.

3.3 Assess Management of Configuration Changes

According to NIST, configuration changes includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for IT products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities.[63] The management of configuration changes begins with the establishment of a formal change management process. Management should authorize and approve all configuration changes. Responsible parties should document and approve test plans as well as develop standards for all levels of testing. Testing should be comprehensive and appropriately consider security and impacts on interfacing systems. Configuration changes should also be clearly documented and tracked.

Generally, system and information owners have the primary responsibility for authorizing system changes based on user input; however, these proposed changes should be discussed with system developers to confirm each change is feasible and cost effective. For this reason, an organization may require a senior systems developer to co-authorize all system changes. The use of standardized change request forms helps ensure that requests are clearly communicated and approvals are documented. Configuration management authorization documentation should be maintained for at least as long as a system is in operation in the event that questions arise regarding why or when system modifications were made.

A disciplined process for testing and approving new and modified systems before their implementation is essential to make sure systems' hardware and related programs operate as intended and that no unauthorized changes are introduced. Test plans should appropriately consider security. The extent of testing varies depending on the type of modification. For new systems being developed or major system enhancements, testing would be extensive, progressing from individual program modules (unit) to groups of modules that must work together (integration) to an entire system (system). Minor modifications may require less extensive testing; however, changes should still be carefully controlled and approved since relatively minor program code changes can have a significant impact on security and overall data reliability.

The configuration management plan should identify each level of decision-making and authority for approving proposed system changes and its management of development and production baselines. A configuration status accounting process should include recording and reporting the status of configuration items. The minimum data elements to be tracked for a configuration item are (1) its initial approved version, (2) the status of requested changes, and (3) the implementation status of approved changes. The level of detail and specific data required may vary according to the organization's needs.

Control Objectives and Audit Procedures

Key practice 3.3 in the Chapter 3 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's management of configuration changes.

[63] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

3.4 Assess Configuration Monitoring Activities

According to NIST, configuration monitoring activities are used as the mechanism to validate that the system is adhering to organizational policies, procedures, and the approved secure baseline configuration.[64] Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system. IT products should comply with applicable standards and the vendors' approved security practices. The organization should have the capability to monitor and test that the configuration of the hardware, software, and firmware is functioning as intended. Also, networks should be appropriately configured and monitored to adequately protect access paths between information systems.

An important part of configuration monitoring are configuration assessments. Configuration assessments establish that the design has achieved the functional and performance requirements as defined in the configuration documentation. These assessments also ensure that the documentation has accurately described the design. The configuration plan should also identify the frequency of these assessments.

Control Objectives and Audit Procedures

Key practice 3.4 in the Chapter 3 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's configuration monitoring activities.

3.5 Assess Software Update Process

According to NIST,[65] the software update process ensures software is scanned and updated frequently to guard against known vulnerabilities.[66] In addition to periodically looking for software vulnerabilities and fixing them, security software should be kept current by establishing effective programs for patch management, virus protection, and other emerging threats.

Vulnerability scanning. Using appropriate vulnerability scanning tools and techniques, an organization's management should scan for vulnerabilities in the information system or when significant new vulnerabilities affecting the system are identified and reported.

Patch management. Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack.[67] It includes acquiring, testing, applying, and monitoring patches to a computer system. According to NIST, patch management helps prevent compromises, data breaches, operational disruptions, and other adverse events.[68]

Virus protection. Protecting information systems from malicious computer viruses and worms is a serious challenge.[69] Computer attack tools and techniques are becoming increasingly sophisticated. Viruses are

[64] National Institute of Standards and Technology, *Guide for Security-Focused Configuration Management of Information Systems*, SP 800-128 (Gaithersburg, MD: August 2011).

[65] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[66] Organizations should also ensure software is supported by the vendor and up to date.

[67] Patch management is the process of applying software patches to correct flaws. A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

[68] National Institute of Standards and Technology, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, SP 800-40, Revision 4 (Gaithersburg, MD: April 2022).

[69] Worms and viruses are commonly used to launch denial-of-service attacks, which generally flood targeted networks and systems with so much transmission of data that regular traffic is either slowed or completely interrupted. Unlike computer viruses, worms do not require human involvement to propagate.

spreading faster as a result of the increasing connectivity of today's networks. Further, commercial off-the-shelf products can be easily exploited for attack.

Emerging threats. Entities are facing a set of emerging cybersecurity threats that are the result of changing sources of attack, increasingly sophisticated social engineering techniques designed to trick the unsuspecting user into divulging sensitive information, new modes of covert compromise, and the blending of once distinct attacks into more complex and damaging exploits. Advances in anti-spam measures have caused spammers to increase the sophistication of their techniques to bypass detection. The frequency and sophistication of phishing[70] attacks have likewise increased, and spyware[71] has proven to be difficult to detect and remove. Other emerging threats include the increased sophistication of worms, viruses, and other malware, and the increased attack capabilities of blended threats and botnets.[72]

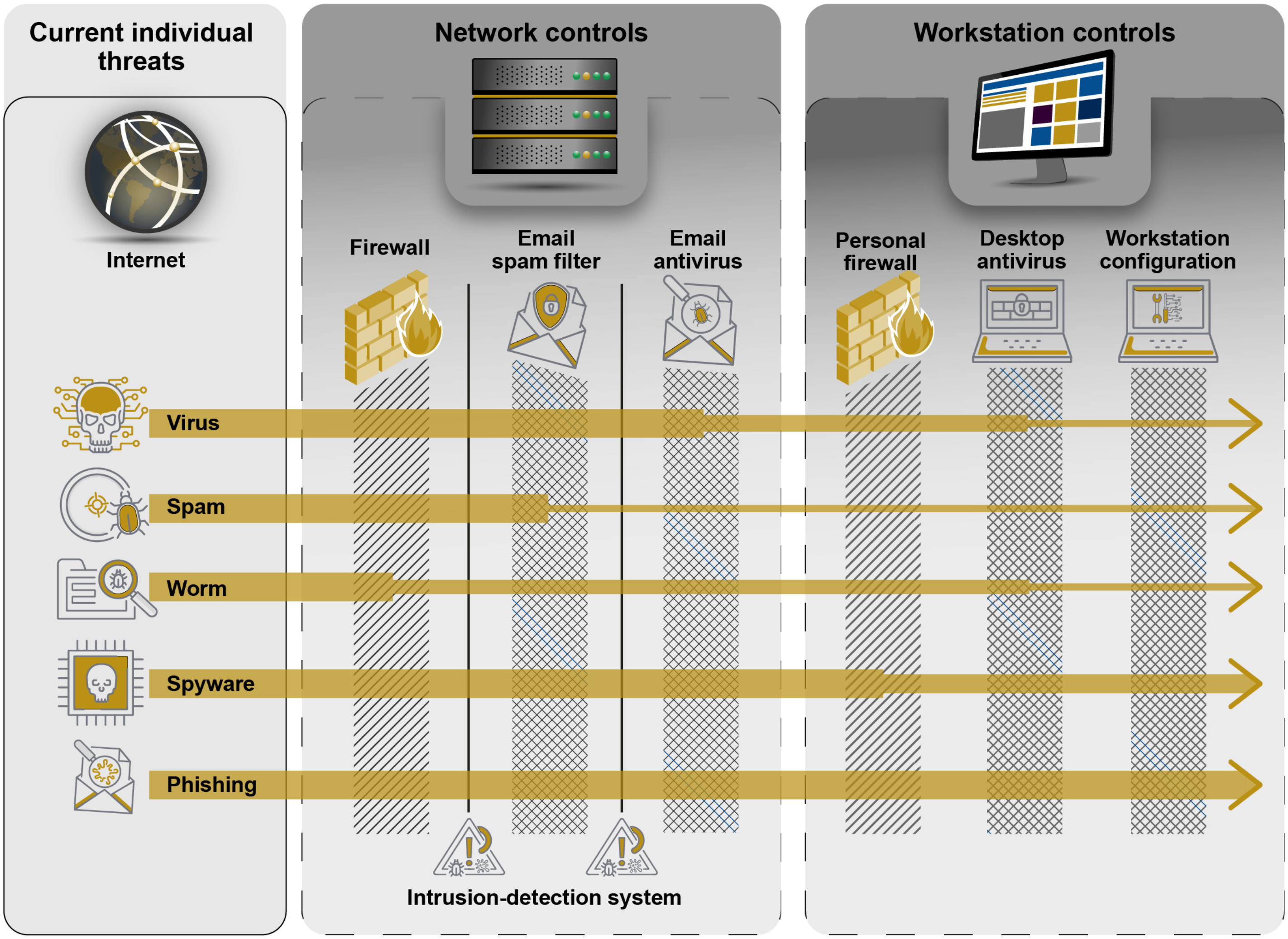
Figure 13 highlights how a layered defense is necessary to protect against these threats.

[70] Phishing is tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

[71] Spyware is software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.

[72] Botnets are compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots) have become a key automation tool to speed infection of vulnerable systems.

Figure 13: The Importance of a Layered Defense against Cyberattacks



Source: GAO; images: GAO and marinashevchenko/stock.adobe.com. | GAO-23-104705

In addition to the threats illustrated in figure 13, the transition to internet protocol version 6 (IPv6) also creates new security risks. The internet protocol provides the addressing mechanism that defines how and where information moves across interconnected networks. The key characteristics of IPv6 are designed to increase address space, promote flexibility and functionality, and enhance security. However, as IPv6-capable software and devices accumulate in organization networks, they could be abused by attackers if not managed properly. Specifically, some existing firewalls and intrusion detection systems do not provide IPv6 detection or filtering capability, and malicious users might be able to send IPv6 traffic through these security devices undetected. Configuration management can mitigate this threat by tightening firewalls to deny direct outbound connections and tuning intrusion detection systems to detect IPv6 traffic.

Similarly, because of the requirement for secure communications, establishing secure voice over internet protocol (VoIP) technologies and networks is a complex process that requires greater effort than that required for data-only networks.[73] For example, typical firewall security configurations need to be re-examined when VoIP systems are implemented because of operational aspects required by this type of system that may in turn reduce the effectiveness of normally applied firewall security configurations. To mitigate this threat, the

[73] VoIP is the routing of voice conversations over the internet or any other internet protocol network.

organization should establish usage restrictions and implementation guidance for VoIP, and document and control the use of VoIP. In addition, the organization should establish monitoring and review procedures to ensure security effectiveness.

Control Objectives and Audit Procedures

Key practice 3.5 in the Chapter 3 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's software update process.

3.6 Review Documentation on Emergency Configuration Changes

According to NIST, situations may arise that necessitate an emergency change.[74] Because of the increased risk that errors or other unauthorized modifications could be implemented, emergency changes should be kept to a minimum. It is important that an organization follow established procedures to perform emergency software changes and reduce the risk of suspending or abbreviating normal controls. Generally, emergency procedures should specify when emergency software changes are warranted, who may authorize emergency changes, how emergency changes are to be documented, and within what period after implementation the change must be tested and approved.

Making emergency changes often involves using sensitive system utilities or access methods that grant much broader access than would normally be needed. It is important that such access is strictly controlled and that their use be promptly reviewed. Shortly after an emergency change is made, the usual configuration management controls should be applied retroactively. That is, the change should be subjected to the same review, testing, and approval process that apply to scheduled changes. In addition, logs of emergency changes and related documentation should be periodically reviewed by data center management or security administrators to determine whether all changes have been tested and received final approval.

Control Objectives and Audit Procedures

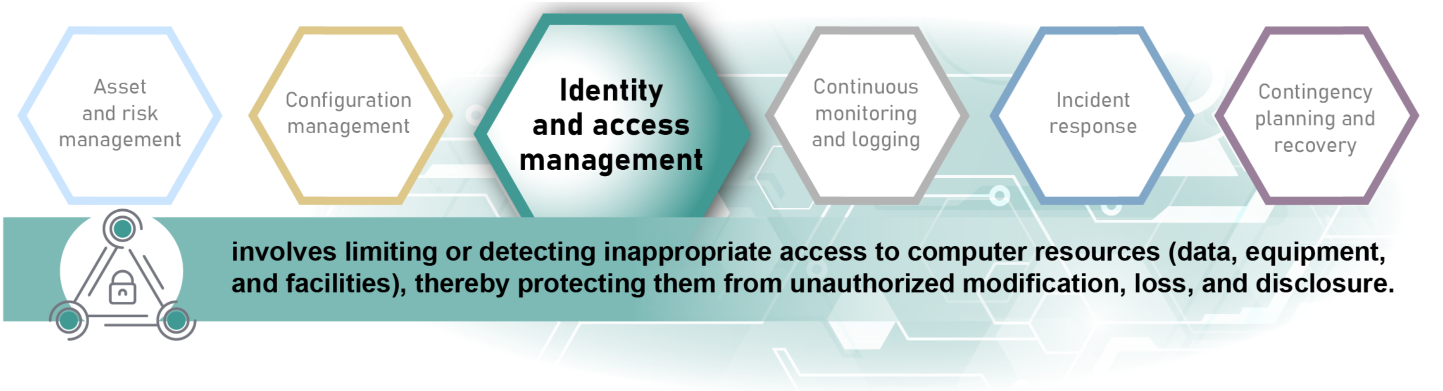
Key practice 3.6 in the Chapter 3 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's documentation on emergency configuration changes.

[74] National Institute of Standards and Technology, *Guide for Security-Focused Configuration Management of Information Systems*, SP 800-128 (Gaithersburg, MD: August 2011).

4 Identity and access management

Source: GAO; images: Murrstock/stock.adobe.com, marinashevchenko/stock.adobe.com and ixtumz88/stock.adobe.com. | GAO-23-104705

Chapter 4. Identity and Access Management Audit Steps


Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery
involves limiting or detecting inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure.

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

4. Identity and Access Management

.

Key Practices in This Chapter

4.1 Evaluate system boundary protection: determine the extent to which the organization protects the logical or physical boundary around a set of information resources and implements measures to prevent unauthorized information exchange across the boundary in either direction.

4.2 Assess identification and authentication mechanisms: determine the extent to which the organization effectively uses authentication mechanisms to identify and authorize the appropriate resources to users.

4.3 Assess data protection and privacy activities: determine the extent to which the organization effectively protects privacy information consistent with relevant laws and guidance.

4.4 Review the security policies on hiring, transfer, termination, and performance: determine the extent to which that the organization has enacted the appropriate personnel and human resources policies and procedures.

Note: The use of "should" statements within key practices does not indicate a requirement unless explicitly stated in criteria. Auditors using this guide should apply professional judgment when determining which key practices and audit steps to implement.

Examples of Criteria to Consider

In addition to the criteria discussed in the “Identify Criteria” section of this guide, consider the following:

NIST, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, FIPS 201-3 (Gaithersburg, MD: January 2022): establishes a standard for a personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive (HSPD)-12.

NIST, *Resilient Interdomain Traffic Exchange: Border Gateway Protocol (BGP) Security and Denial of Service (DDoS) Mitigation,* SP 800-189 (Gaithersburg, MD: December 2019): provides guidelines and recommendations for deploying protocols that improve the security of interdomain traffic exchange.

NIST, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* – SP 800-60, Revision 1 (Gaithersburg, MD: August 2008): contains the basic guidelines for mapping types of information and information systems to security categories.

OMB, *Memorandum for Heads of Executive Departments and Agencies: Update to the Trust Internet Connections (TIC) Initiative* M-19-26 (Washington, D.C.: September 2019): provides an approach for federal organizations to implement the Trust Internet Connections initiative with increased flexibility to use modern security capabilities.

OMB, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management,* M-19-17 (Washington, D.C.: May 21, 2019): provides policy-level guidance for federal organizations to identify, credential, monitor, and manage user access to information and information systems and adopt sound processes for authentication and access control.

OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* M-03-22 (Washington, D.C.: Sept. 26, 2003): directs federal organizations to conduct reviews of how information about individuals is handled within their agencies when they use IT to collect new information, or when organizations develop or buy new IT systems to handle collection of PII.

DHS, *Policy for a Common Identification Standard for Federal Employees and Contractors*, HSPD-12 (Jan. 27, 2022): mandates a federal standard for secure and reliable forms of identification.

4.1 Evaluate System Boundary Protection

According to NIST, boundary protection is the monitoring and control of communications at the external interface to a system to prevent and detect malicious and other unauthorized communications using boundary protection devices.[75] Firewall devices represent the most common boundary protection technology at the network level. At the organizational level, access control policy is developed and promulgated through procedures, manuals, and other guidance. At the system level, any connections to the internet, or to other external and internal networks or information systems, should occur through controlled interfaces. At the host or device level, logical boundaries can be controlled through inbound and outbound filtering provided by access control lists and personal firewalls. At the application level, logical boundaries to business process applications may be controlled by access control lists in security software or within the applications.

Control Objectives and Audit Procedures

Key practice 4.1 in the Chapter 4 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's protection of information system boundaries. These are a sample of controls and not the only controls that should be considered. Professional judgment should be used to determine which controls are appropriate for the audited organization. Additionally, these audit procedures should be considered for systems under the control of the organization. For example, these procedures may not apply to systems owned or managed by a contractor or other third-party.

4.2 Assess Identification and Authentication Mechanisms

According to NIST, identification and authentication mechanisms prevent unauthorized people (or unauthorized processes) from entering a computer system.[76] If logical connectivity is allowed, then the system identifies and authenticates (1) users, (2) processes acting on behalf of users, (3) services, and (4) specific devices. Users' identities may be authenticated through something they know (a traditional password), something they have (such as a token or card), or something about them that identifies them uniquely (such as a fingerprint). Multi-factor authentication is a mechanism to verify an individual's identity by utilizing two or more of these elements. For example, in addition to a password, a user may be required to enter a code to verify their identity. Executive Order 14028 requires that federal organizations utilize multi-factor authentication.[77]

4.2.1 Assess Logical Access Controls

The organization's management should ensure that there are logical access controls over sensitive system resources to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage. If authentication is successful, authorization determines what users can do (i.e., it grants or restricts user, service, or device access to various network and computer resources based on the identity of the user, service, or device).

Control Objectives and Audit Procedures

Key practice 4.2 in the Chapter 4 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's identification and authentication mechanism.

[75] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

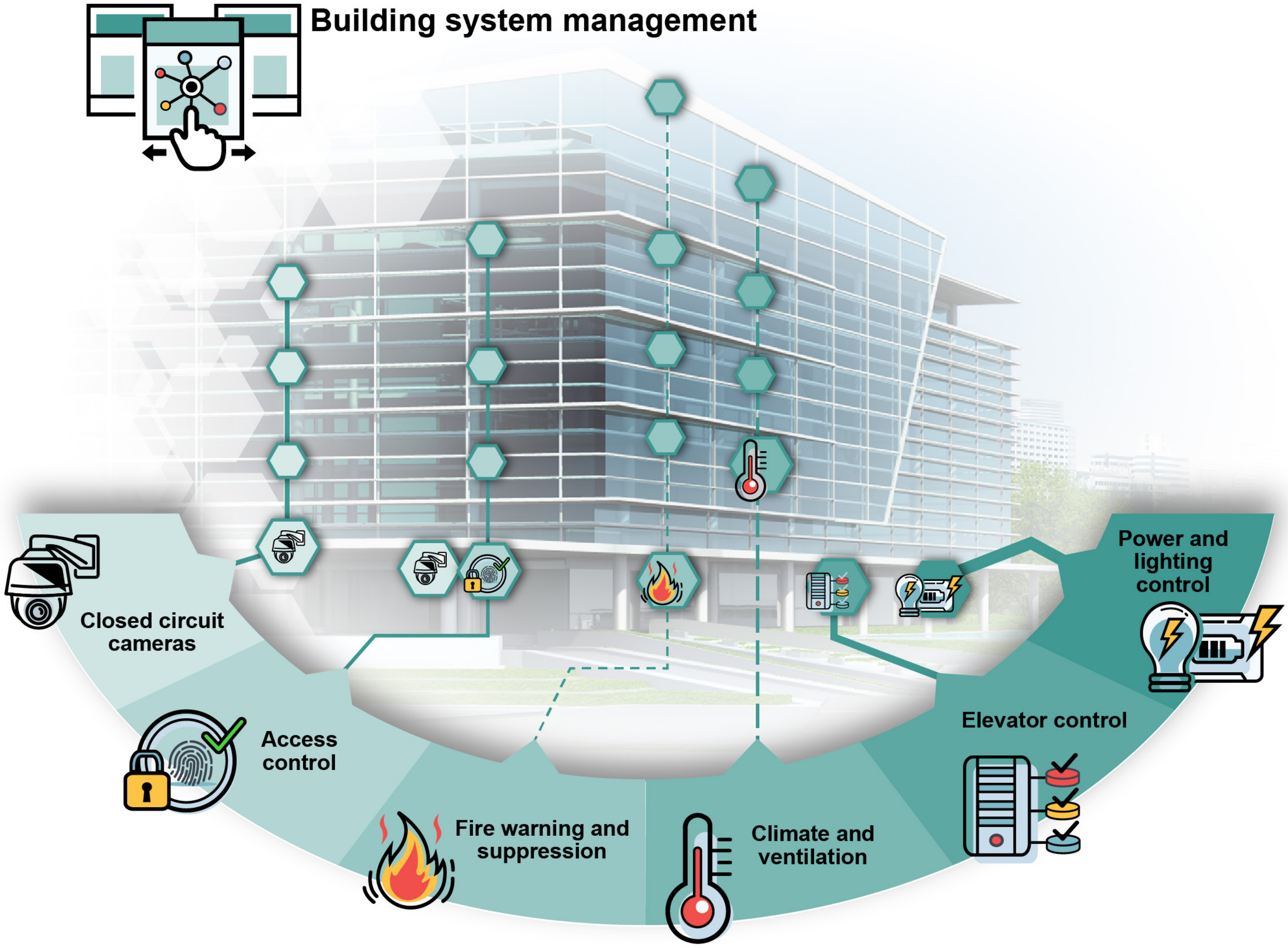
[76] National Institute of Standards and Technology, *An Introduction to Information Security*, SP 800-12, Revision 1 (Gaithersburg, MD: June 2017).

[77] The White House, *Executive Order on Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

4.2.2 Assess Physical Access Controls

Moreover, the organization's management should ensure that there are physical access controls over sensitive system resources. Physical security controls restrict physical access or harm to computer resources and protect these resources from intentional or unintentional loss or impairment. Such controls include guards, gates, and locks, and environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies. See figure 14 for an illustrated example of physical security controls.

Figure 14: Monitoring, Locks, and Power and Environmental Control Systems Provide IT Security


Building system management
Closed circuit cameras
Access control
Fire warning and suppression
Climate and ventilation
Elevator control
Power and lighting control

Source: GAO; images: archipoch/stock.adobe.com, Buffaloboy/stock.adobe.com and koson_thamai/stock.adobe.com. | GAO-23-104705

Control Objectives and Audit Procedures

Key practice 4.2 in the Chapter 4 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's identification and authentication mechanisms.

4.3 Assess Data Protection and Privacy Activities

Organizations should consider the risks associated with sensitive privacy information which includes data protection and privacy activities. Federal agencies are subject to privacy laws aimed at preventing the misuse of PII. The *Privacy Act of 1974 (Privacy Act)* and the privacy provisions of the *E-Government Act of 2002 (E-Government Act)* contain requirements for the protection of personal privacy by federal agencies.[78] The *Privacy Act* places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[79] The act also requires that when agencies establish or make changes to a system of records, they must notify the public by a "system of records notice."[80] The *E-Government Act* strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments. These assessments include an analysis of how personal information is collected, stored, shared, and managed in a federal system. According to OMB, privacy impact assessments must analyze and describe how the information will be secured, including administrative and technological controls. Additionally, these assessments should be kept up to date.[81]

According to NIST, in establishing confidentiality impact levels for each information type, responsible parties must consider the consequences of unauthorized disclosure of privacy information.[82] NIST states, in most cases, the impact on confidentiality for private information will be in the moderate range.[83]

Organizations should also consider the adequacy of their efforts to protect data stored or processed by their systems. According to NIST, problems can arise where there is a loss of confidentiality, integrity, or availability at some point in the data processing, such as data theft by external attackers or the unauthorized access or use of data by employees.[84] Accordingly, NIST has established guidelines and controls for doing so. This includes employing principles such as:

- separation of duties— designed to address the potential for abuse of authorized privileges and helps reduce the risk of malevolent activity without collusion;
- least privilege—intended to ensure that individuals or systems are granted the minimum system resources and authorizations necessary to perform their function; or

[78] 5 U.S.C. § 552a E-Government Act of 2002, Title II, Sec. 208, Pub. L. 107-347, 116 Stat. 2899, 2921 (Dec. 17, 2002), codified at 44 U.S.C. § 3541, et seq3501 note.

[79] 5 U.S.C. § 552a.The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also identifies "system of records" as a group of records under the control of any agency retrieved by the name of the individual or by an individual identifier.

[80] 5 U.S.C. § 552a(e)(4). A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by a federal agency. Agencies must publish SORNs in the Federal Register.

[81] See OMB Memorandum M-03-22: *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Washington, DC: Sept. 26, 2003) (identifying the requirements of what a privacy impact assessment must contain). Also, according to *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB Memorandum M-06-20, July 17, 2006, a privacy impact assessment or a system of records notice is current if that document satisfies the applicable requirements and subsequent substantial changes have not been made to the system.

[82] NIST, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories,* SP 800-60, Revision 1 (August 2008).

[83] The standard defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

[84] National Institute of Standards and Technology, *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Gaithersburg, MD: January 2020).

- cryptographic key management—used to secure network storage and communication.

For example, to address the confidentiality and integrity of data, organizations should employ encryption mechanisms for the data, both at rest and in transit. According to NIST, media sanitization is a critical element to maintain data confidentiality.[85] Organizations need to exercise proper control on confidential information to avoid data leakage due to improper disposal of storage media or improperly wiped refurbished media.

Control Objectives and Audit Procedures

Key practice 4.3 in the Chapter 4 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's data protection and privacy activities.

4.4 Review the Security Policies on Hiring, Transfer, Termination, and Performance

According to NIST, policies related to personnel actions, such as hiring, termination, and employee expertise, are important considerations in securing information systems.[86] If personnel policies are not adequate, an organization runs the risk of (1) hiring unqualified or untrustworthy individuals; (2) providing terminated employees opportunities to sabotage or otherwise impair organization operations or assets; (3) failing to detect continuing unauthorized employee actions; (4) lowering employee morale, which may in turn diminish employee compliance with controls; and (5) allowing staff expertise to decline.

Where appropriate, termination and transfer procedures should include exit interview procedures, return of property (e.g., keys, identification cards, badges, and passes), prompt termination of access to the organization's resources and facilities (including passwords), and identification of the period during which nondisclosure requirements remain in effect.

Control Objectives and Audit Procedures

Key practice 4.4 in the Chapter 4 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's security policies on hiring, transfer, termination, and performance.

[85] National Institute of Standards and Technology, *Guidelines for Media Sanitization,* Revision 1.0 (Gaithersburg, MD: December 2014).

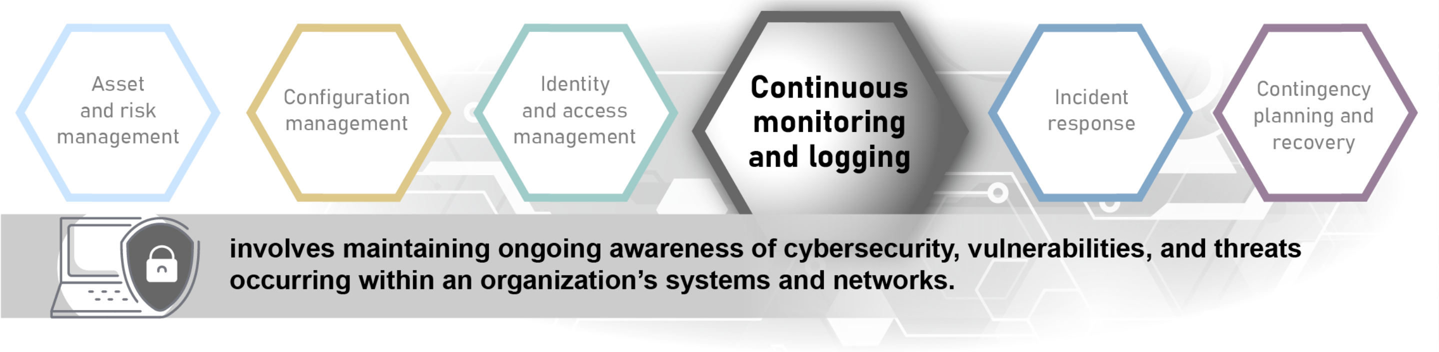
[86] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: April 2018).

Continuous monitoring and logging

5

Source: GAO; images: Tobias/stock.adobe.com, marinashevchenko/stock.adobe.com and ixtumz88/stock.adobe.com. | GAO-23-104705

Chapter 5. Continuous Monitoring and Logging Audit Steps


Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery

involves maintaining ongoing awareness of cybersecurity, vulnerabilities, and threats occurring within an organization's systems and networks.

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

5. Continuous Monitoring and Logging

.

Key Practices in This Chapter

5.1 Assess continuous monitoring: determine the extent to which the organization regularly collects and monitors security events for indications of inappropriate or unusual activity.

5.2 Review the continuous monitoring strategy and implementation: determine the extent to which the organization's ongoing awareness of its system security and privacy posture supports organizational risk management decisions.

5.3 Review security control assessments and assessor independence: determine the extent to which the organization's security and privacy controls are meeting stated goals and objectives, including the use of an independent assessor.

5.4 Review automated monitoring results: determine the extent to which the organization has an efficient and effective approach to accomplish continuous monitoring.

5.5 Assess security event identification, logging, and retention: determine the extent to which the organization's significant security events are identified, logged, and retained, as appropriate.

Note: The use of "should" statements within key practices does not indicate a requirement unless explicitly stated in criteria. Auditors using this guide should apply professional judgment when determining which key practices and audit steps to implement.

Examples of Criteria to Consider

In addition to the criteria discussed in the “Identify Criteria” section of this guide, consider the following:

NIST, *Automation Support for Security Control Assessments: Volume 1: Overview*, NISTIR 8011 Volume 1 (Gaithersburg, MD: June 2017): introduces concepts to support automated assessment of most of the security controls in NIST SP 800-53.

NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, SP 800-137 (Gaithersburg, MD: September 2011): provides guidelines to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program.

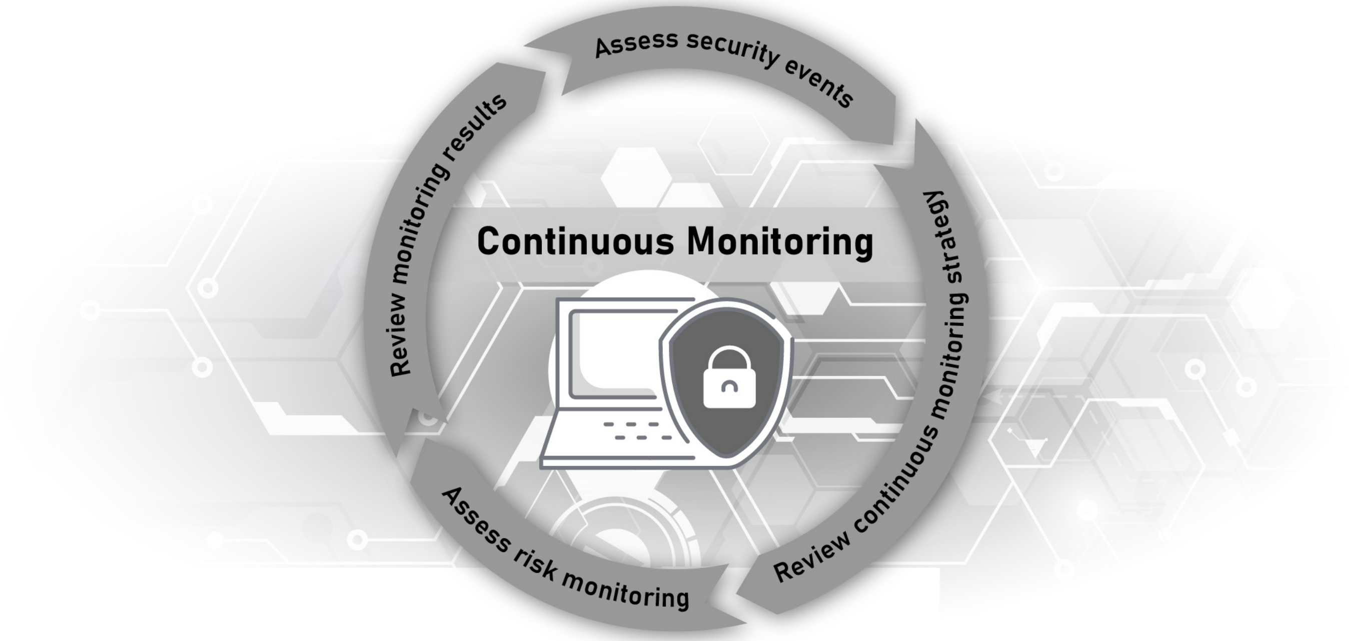
NIST, *Guide to Computer Security Log Management*, SP 800-92 (Gaithersburg, MD: September 2006): provides guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise.

OMB, *Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31(Washington, D.C.: Aug. 27, 2021): addresses the requirements in section 8 of Executive Order 14028 for logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center of each agency.

5.1 Assess Continuous Monitoring

According to NIST, continuous monitoring is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[87] Continuous monitoring involves the regular collection and monitoring of security events for indications of inappropriate or unusual activity. Continuous monitoring supports the requirements found in FISMA and OMB Circular A-130.[88] OMB Circular A-130 requires federal organizations to develop continuous monitoring strategies and to implement continuous monitoring activities. Figure 15 summarizes the continuous monitoring process as defined by NIST.

Figure 15: Continuous Monitoring Life Cycle for Cybersecurity Events



Source: GAO analysis of National Institute of Standards and Technology SP 800-137; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

Continuous monitoring is a critical part of the risk management process. Additionally, an organization's overall security architecture and accompanying security program should be monitored to ensure that organization-wide operations remain within an acceptable level of risk, despite any changes that can occur. Therefore, having timely, relevant, and accurate information is vital. Since resources are usually limited, organizations must prioritize their efforts. This information will help with timely risk management decisions, including authorization decisions.[89]

According to OMB A-130, continuous monitoring includes, but is not limited to, assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organization officials on an ongoing basis.[90] Failing to implement a sufficient continuous monitoring program can significantly affect an

[87] National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* SP 800-37 (Gaithersburg, MD: September 2011).

[88] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

[89] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, SP 800-37, Revision 2 (Gaithersburg, MD: December 2018).

[90] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

organization’s ability to accomplish its mission. If continuous monitoring controls are inadequate, officials will not have sufficient knowledge of the security state of the system to determine whether continued operation was acceptable based on ongoing risk. DHS initiated the Continuous Diagnostics and Mitigation (CDM) program to provide federal agencies with access to continuous monitoring sensors, diagnosis, mitigation tools, and dashboards. Effective use of these capabilities can strengthen the security posture of government networks.[91]

According to NIST, organizations should increase their situational awareness through enhanced monitoring capabilities in analyzing network traffic at external boundaries and inside their internal network to identify anomalous, inappropriate, malicious, or unusual activities.[92] Situational awareness should include developing a capability to analyze network traffic data over an extended period of time. Further, intrusion detection systems (IDS) can detect attacks and indicators of potential attack, unauthorized network connections, and unauthorized use of information systems.

Control Objectives and Audit Procedures

Key practice 5.1 in the Chapter 5 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization’s continuous monitoring. These are a sample of controls and not the only controls that should be considered. Professional judgment should be used to determine which controls are appropriate for the audited organization. Additionally, these audit procedures should be considered for systems under the control of the organization. For example, these procedures may not apply to systems owned or managed by a contractor or other third-party.

5.2 Review the Continuous Monitoring Strategy and Implementation

According to NIST, any effort or process intended to support continuous monitoring begins with defining a continuous monitoring strategy.[93] The organization should develop a system-level continuous monitoring strategy and implement the monitoring in accordance with the strategy. Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. A well-designed continuous monitoring strategy encompasses security status monitoring, control assessments, and status reporting in support of timely risk-based decision-making throughout the organization.

Continuous monitoring programs also allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards provides organizational officials with the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Further, as previously discussed in Chapter 2, the risk environment, risk management program, and associated activities should be assessed to support risk decisions. Risk monitoring is an important part of an organization’s continuous monitoring strategy. According to NIST, risk monitoring involves maintaining ongoing awareness of an organization’s risk environment, risk management program, and associated activities to support risk decisions.[94] Ensuring that risk monitoring is an integral part of the continuous monitoring strategy

[91] https://www.cisa.gov/cdm.

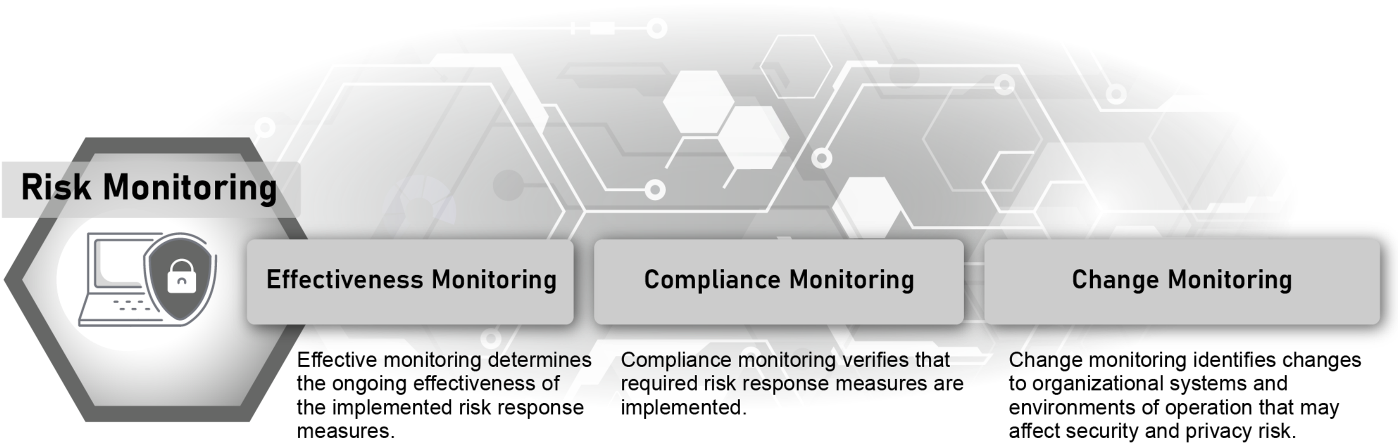
[92] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[93] NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* SP 800-137 (Gaithersburg, MD: September 2011).

[94] NIST*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* SP 800-137 (Gaithersburg, MD: September 2011).

includes activities such as effectiveness monitoring, compliance monitoring, and change monitoring (see figure 16).

Figure 16: Types of Monitoring Performed as Part of the Risk Monitoring Process



Effective monitoring determines the ongoing effectiveness of the implemented risk response measures.

Compliance monitoring verifies that required risk response measures are implemented.

Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Source: GAO analysis of National Institute of Standards and Technology continuous monitoring guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

Control Objectives and Audit Procedures

Key practice 5.2 in the Chapter 5 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization’s continuous monitoring strategy and implementation.

5.3 Review Security Control Assessments and Assessor Independence

According to NIST, security control assessments are the testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly and operating as intended. They also verify that implemented security and privacy controls are meeting their stated goals and objectives. These assessments are an essential element of any continuous monitoring strategy. According to NIST, as part of the control assessment process, organizations are required to designate appropriate internal and/or independent third party assessors, develop control assessment plans that are reviewed and approved by management, access the selected controls, produce a control assessment report, and provide the results to organizationally defined personnel.

Assessor independence is an essential element of an effective continuous monitoring and control assessment process. To maintain independence, assessors should not have a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, or place themselves in advocacy positions for the organizations acquiring their services. OMB Circular A-130 requires that organizations perform an independent evaluation of the information security programs and practices to determine their effectiveness.[95] Further, NIST SP 800-53A *Assessing Security and Privacy Controls in Information Systems and Organizations* contains control assessments and potential assessment methods for independent assessors.[96]

[95] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

[96] National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Information Systems and Organizations*, SP 800-53, Revision 5 (Gaithersburg, MD: January 2022).

Independence provides assurance that the results are sound and can be used to make credible, risk-based decisions. The appropriate level of independence is determined by authorizing officials based on, among other things, the security category of the system and risk to the organization's operations, assets, and individuals.

Control Objectives and Audit Procedures

Key practice 5.3 in the Chapter 5 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's security control assessments and assessor independence.

5.4 Review Automated Monitoring Results

According to NIST, automation is an efficient and effective way to accomplish continuous monitoring. Automation supports more frequent updates to hardware, software, and firmware inventories; authorization packages; and other system information.[97] Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely.

Automating control assessments is a fundamental element in helping organizations manage information. According to NIST, security-related information should be generated, correlated, analyzed, and reported using automated tools (e.g., vulnerability scanning tools and network scanning devices) to the extent that it is possible and practical to do so.[98] Using automated tools for continuous monitoring helps to maintain the accuracy, currency, and availability of information. This in turns helps to increase the level of ongoing awareness of the organization's security and privacy posture.

Components of information integrity supported via automated monitoring tools include the following:

- Accuracy – degree to which the data reflect the reality
- Currency – degree to which the data are recent
- Availability – degree to which the data are available for use when needed

When it is not feasible to use automated tools, security-related information can be generated, correlated, analyzed, and reported using manual or procedural methods.

To help federal organizations automate ongoing security assessments, NIST and CISA have collaborated on the development of a CDM-based process. The CDM-based process leverages the test assessment method from NIST 800-53A[99] and is intended to be consistent with the NIST risk management framework, as described in SP 800-37 and the information security continuous monitoring guidance in SP 800-137.[100]

[97] NIST*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* SP 800-137 (Gaithersburg, MD: September 2011).

[98] National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, SP 800-137 (Gaithersburg, MD: September 2011).

[99] For more information on the test assessment method, see https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final.

[100] National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* SP 800-37 (Gaithersburg, MD: September 2011).

Through this process, the CISA CDM program facilitates automation of the test method for security assessments. These assessments can be used as part of a broader ongoing authorization program.[101]

Control Objectives and Audit Procedures

Key practice 5.4 in the Chapter 5 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's automated monitoring results.

5.5 Assess Security Event Identification, Logging, and Retention

As previously mentioned, the organization's policies and procedures should establish criteria for the identification of significant system events that should be logged. Executive Order 14028 establishes requirements for logging, log retention, and log management. At a minimum, all such significant events, including access to and modification of sensitive or critical system resources, should be logged.[102] To be effective:

- identification and logging of auditable events should be based on considerations of costs, benefits, and risk;
- the automated system should be activated to log critical activity, maintain critical audit trails, and report unauthorized or unusual activity;
- access to audit logs should be adequately controlled; and
- managers should review logs for unusual or suspicious activity and take appropriate actions.

If an organization has insufficient logging, it will face an increased risk of not having the information needed to investigate performance issues and suspicious activity. NIST states that organizations should include an automated centralized logging analysis capability, such as from security information and event management technologies that can produce real-time alerts, notifications, and follow-up of significant security events generated by information systems.[103] Security information and event management logs should be used to support organizations after the security investigations including forensic analysis, establishing baselines, and identifying operational trends and long-term problems.

The completeness and value of the audit trails maintained will only be as good as the organization's ability to thoroughly identify the critical processes and the related information that may be needed. Procedures for maintaining such audit trails should be based on

- the value or sensitivity of data and other resources affected,
- the processing environment (e.g., systems development, testing, or production),

[101] For more information on CISA and the CDM program, see https://www.cisa.gov/cdm | https://www.dhs.gov/topic/cybersecurity | https://www.cisa.gov/einstein | https://www.cisa.gov/hva-pmo | https://www.cisa.gov/national-cybersecurity-protection-system-ncps | https://www.cisa.gov/network-security-deployment | https://www.cisa.gov/situational-awareness-and-incident-response |https://www.cisa.gov/trusted-internet-connections.

[102] The White House, *Executive Order on Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[103] Security information and event management technology is defined as an application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface. National Institute of Standards and Technology, *Guide for Security-Focused Configuration Management of Information Systems*, SP 800-128 (Gaithersburg, MD: August 2011).

- technical feasibility, and
- legal and regulatory requirements.

Audit trails, including automated logs, need to be retained for an appropriate period of time. An effective IDS should also be implemented, including appropriate placement of intrusion detection sensors and setting of incident thresholds. IDS security software generally provides a means of determining the source of a transaction or an attempted transaction and of monitoring users' activities (audit trail).

According to NIST, logs of security events should also be stored for an appropriate period of time in accordance with regulatory requirements (e.g., National Archives and Records Administration records management schedule) and should contain sufficient details.[104] The records management schedule states that security incident data should be retained for at least 3 years.[105]

Control Objectives and Audit Procedures

Key practice 5.5 in the Chapter 5 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's security event identification, logging, and retention.

[104] National Institute of Standards and Technology, *Guide to Computer Security Log Management*, SP 800-92 (Gaithersburg, MD: September 2006).

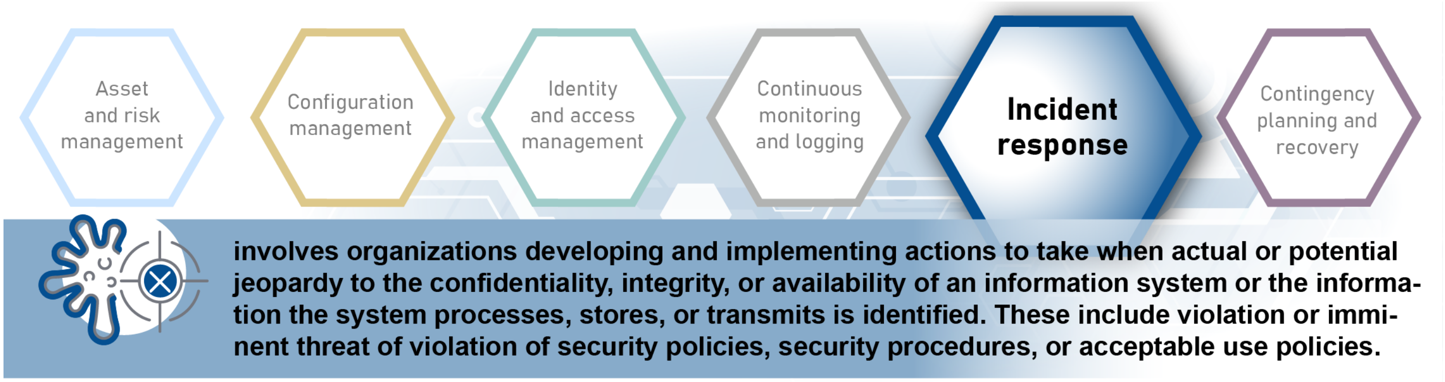
[105] National Archives and Records Administration, *General Records Schedule 3.2: Information Systems Security Records*, Transmittal 33 (Washington, D.C.: January 2023). Organizations are to keep incident handling, reporting, and follow-up records for 3 years after all necessary follow-up actions have been completed.

Incident response

6

Source: GAO; images: ArtemisDiana/stock.adobe.com, marinashevchenko/stock.adobe.com and ixtumz88/stock.adobe.com. | GAO-23-104705

Chapter 6. Incident Response Audit Steps


Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery

involves organizations developing and implementing actions to take when actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits is identified. These include violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

6. Incident Response

Key Practices in This Chapter

6.1 **Assess incident response policies, plans, and procedures:** determine the extent to which the organization has codified effective policies, procedures, and plans.

6.2 **Assess incident response capabilities:** determine the extent to which the organization can effectively test incident response capabilities, respond and report on incidents, assist impacted parties, and respond to information spillage.

6.3 **Assess incident response training and testing capabilities:** determine the extent to which organizational personnel have sufficient knowledge, skills, and abilities to complete their assigned incident response and recovery responsibilities, and perform periodic incident response testing.

6.4 **Assess incident monitoring capabilities:** determine the extent to which the organization can effectively track and document information system security incidents.

Note: The use of "should" statements within key practices does not indicate a requirement unless explicitly stated in criteria. Auditors using this guide should apply professional judgment when determining which key practices and audit steps to implement.

Examples of Criteria to Consider

In addition to the criteria discussed in the “Identify Criteria” section of this guide, consider the following:

NIST, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops,* SP 800-83 Revision 1 (Gaithersburg, MD: July 2013): provides recommendations for improving an organization’s malware incident prevention measures and for enhancing an organization’s existing incident response capability so that it is better prepared to handle malware incidents.

NIST, *Computer Security Incident Handling Guide*, SP 800-61, Revision 2 (Gaithersburg, MD: August 2012): provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

OMB, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirement*, M-23-03 (Washington, D.C.: December 2022): provides updated reporting guidance on a generally annual basis in accordance with FISMA and Executive Order 14028.

OMB, *Preparing for and Responding to a Breach of Personally Identifiable Information,* M-17-12 (Washington, D.C.: January 2017): sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals.

CISA, *Cybersecurity Incident & Vulnerability Response Playbooks* (Washington, D.C.: November 2021): provides operational procedures for planning and conducting cybersecurity incident and vulnerability response activities in federal civilian executive branch agencies, including the collection and preservation of data for incident verification, categorization, prioritization, mitigation, reporting, and attribution.

6.1 Assess Incident Response Policies, Plans, and Procedures

According to NIST, incident response policies, plans, and procedures address controls related to the organizational management of, and compliance with, its incident response capability.[106] As mentioned in Chapter 2, an organization's risk management strategy is an important factor in establishing such policies, plans, and procedures, which contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policies, plans, and procedures. Generally, development of these items at the organization level are preferable and may obviate the need for mission- or system-specific policies, plans, and procedures.

Incident response policy and procedures should address purpose, scope, roles, responsibilities, management commitment and approval, coordination among organizational entities, and compliance with applicable laws, regulations, and standards. Some events may precipitate an update to incident response policy and procedures, such as audit findings, security incidents or breaches, changes to the IT environment, or changes in laws, executive orders, directives, regulations, standards, and guidelines.

Items in policies and procedures for an effective incident response program could include information about:

- prompt centralized reporting and active monitoring of alerts/advisories, such as those distributed by CISA;
- incident response team members with the necessary knowledge, skills, and abilities;
- roles and responsibilities training;
- periodic refresher training;
- active protection against denial of service attacks, including ransomware;
- appropriate incident response assistance and consideration of computer forensics;
- processes and benchmarks for notifying an organization's executive leadership; and
- processes and benchmarks for notifying individuals when PII has been breached.

Further, an effective incident response capability codifies the organization's policies and procedures into an incident response plan that provides a documented roadmap with instructions. An incident response plan documents a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against an organization's systems. For example, an incident response plan may include information about the following:

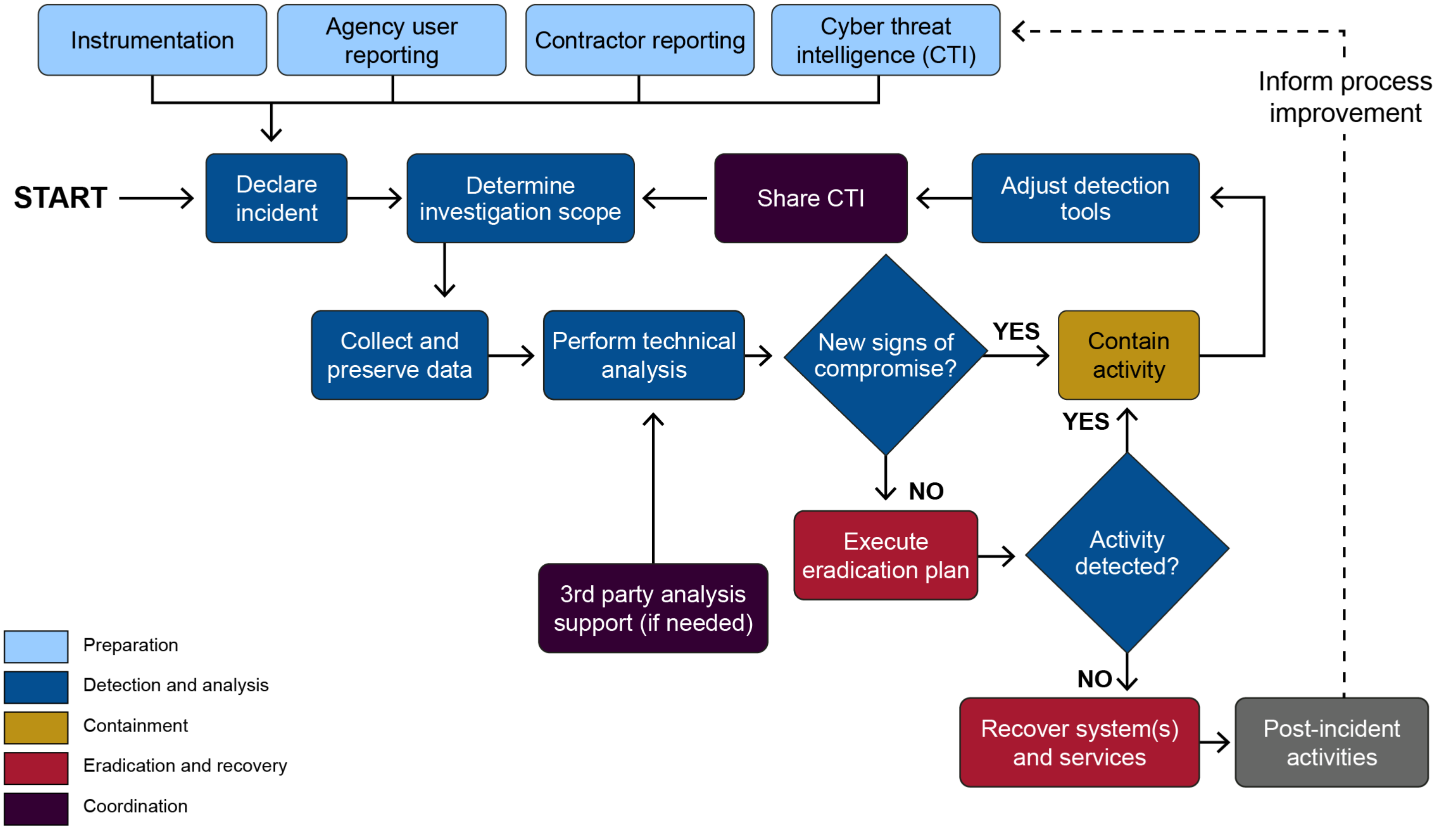
- identifying members of the incident response team;
- analyzing threat logs and other related documentation;
- communicating with external organizations, such as notifying and consulting with, as appropriate, law enforcement organizations, and for federal organizations, relevant organization inspector generals and CISA;
- training for employees;

[106] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

- testing the incident response plan;
- remediating incidents and lessons learned;
- handling incident containment, eradication, and recovery;
- documenting offenses;
- determining the seriousness of violations;
- reporting violations to higher levels of management;
- investigating violations;
- imposing disciplinary action for specific types of violations;
- notifying the resource owner of the violation; and
- sharing incident and threat information with owners of connected systems.

Figure 17 provides a high-level overview of the incident response process.

Figure 17: Cyber Incident Response Process



Source: Cybersecurity and Infrastructure Security Agency, *Cybersecurity Incident and Vulnerability Response Playbooks* (Arlington, VA: November 2021). | GAO-23-104705

Control Objectives and Audit Procedures

Key practice 6.1 in the Chapter 6 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's incident response policies, plans, and procedures. These are a sample of controls and not the only controls that should be considered. Professional judgment should be used to determine which controls are appropriate for the audited organization. Additionally, these audit procedures should be considered for systems under the control of the organization. For example, these procedures may not apply to systems owned or managed by a contractor or other third-party.

6.2 Assess Incident Response Capabilities

According to NIST, effective incident responses are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems.[107] An effective incident handling capability includes coordination among many organizational units (e.g., mission, business, or system owners; authorizing officials; human resources offices; physical and personnel security offices; legal departments; risk executive; operations personnel; and procurement offices).

Incidents should be documented, which includes maintaining records about each incident, the status of the incident, and other pertinent information. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. In addition, POA&Ms that were the result of incidents should be reviewed to ensure corrective actions were taken.

For federal organizations, an incident that involves PII is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence by which an unauthorized user accesses or potentially accesses PII or an authorized user accesses or potentially accesses such information for unauthorized purposes.

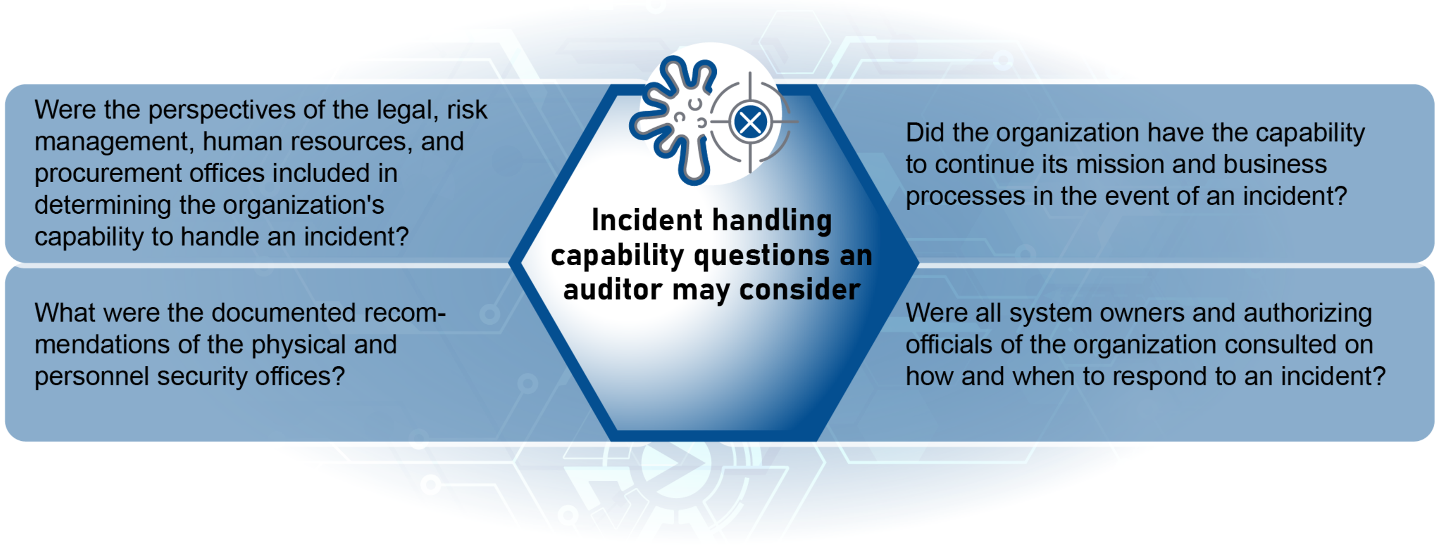
Further, according to NIST, information spillage refers to instances where information is placed on systems that are not authorized to process such information.[108] At that point, corrective action is required. This could include both reviewing documentation of the incident response and interviewing the organization's personnel, including management, to determine the actions that were taken. The nature of the response should be based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with access to the contaminated system. According to NIST, the methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Figure 18 provides a sample of questions that an auditor may consider when determining if an organization has sufficient incident handling capabilities.

[107] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[108] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

Figure 18: Incident Handling Capability Questions Auditors May Consider


Were the perspectives of the legal, risk management, human resources, and procurement offices included in determining the organization's capability to handle an incident?
What were the documented recommendations of the physical and personnel security offices?
Incident handling capability questions an auditor may consider
Did the organization have the capability to continue its mission and business processes in the event of an incident?
Were all system owners and authorizing officials of the organization consulted on how and when to respond to an incident?

Source: GAO; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

Control Objectives and Audit Procedures

Key practice 6.2 in the Chapter 6 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's incident response handling capabilities.

6.3 Assess Incident Response Training and Testing Capabilities

Incident response training helps ensure organizational personnel have sufficient knowledge, skills, and abilities to complete their assigned incident response and recovery responsibilities. According to NIST, this includes ensuring that the appropriate content and level of detail are included in such training.[109] For example, users may only need to know who to call or how identify and report suspicious activities and recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. However, some events may precipitate an update to incident response training content, such as the results of incident response plan testing or response to an actual incident (lessons learned); assessment or audit findings; or changes in applicable laws, executive orders, directives, and regulations.

According to NIST, incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt).[110] Incident response testing can include a determination of the effects on organizational operations, assets, and individuals due to incident response. The organization's incident response testing methods can be assessed by reviewing test schedules, plans, and after-action reports. Additionally, NIST recommends auditors to use qualitative and quantitative data as aids in measuring the effectiveness of incident response testing.

[109] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[110] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

Control Objectives and Audit Procedures

Key practice 6.3 in the Chapter 6 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's incident response training and testing capabilities.

6.4 Assess Incident Monitoring Capabilities

According to NIST SP 800-53, an intrusion detection system (IDS) is software that automates the intrusion detection process.[111] Effective incident monitoring capabilities generally include the use of an IDS. The organization should have an effective IDS in place, including appropriate placement of intrusion detection sensors and setting of incident thresholds. IDS security software generally provides a means of determining the source of a transaction or an attempted transaction and of monitoring users' activities (audit trail).

Because all of the audit trail and log information maintained is likely to be too voluminous to review on a routine basis, IDS security software should be implemented to selectively identify unauthorized, unusual, and sensitive access activity, such as

- attempted unauthorized logical and physical access,
- access trends and deviations from those trends,
- access to sensitive data and resources,
- highly sensitive privileged access, such as the ability to override security controls,
- access modifications made by security personnel, and
- unsuccessful attempts to logon to a system.

As previously discussed in Chapter 5, logging is an important aspect of monitoring which is also an essential part of incident response. Organization policies and procedures should establish criteria for the identification of significant system events that should be logged.

Control Objectives and Audit Procedures

Key practice 6.4 in the Chapter 6 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's incident monitoring capabilities.

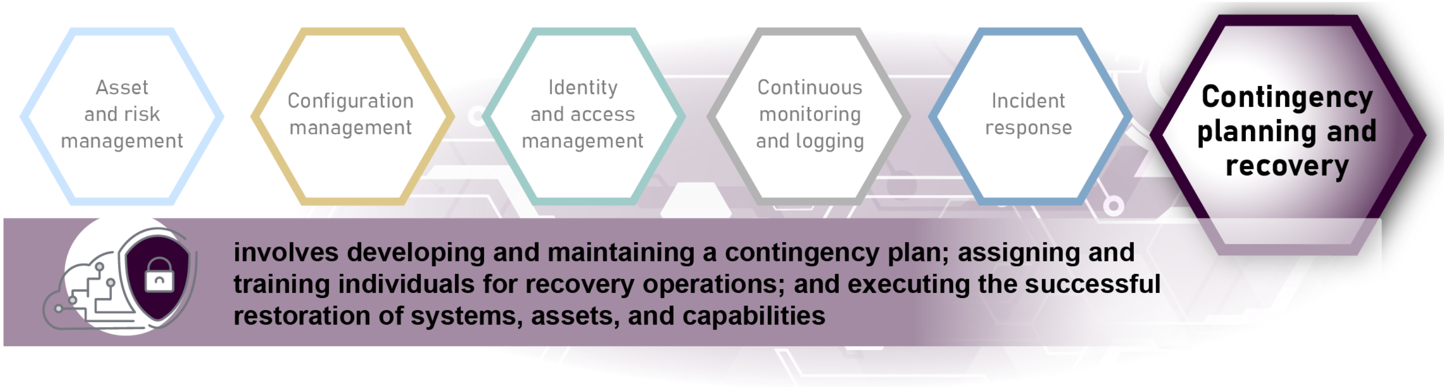
[111] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

Contingency planning and recovery

7

Source: GAO; images: Deemerwha studio/stock.adobe.com, marinashevchenko/stock.adobe.com and ixtumz88/stock.adobe.com. | GAO-23-104705

Chapter 7. Contingency Planning and Recovery Audit Steps


Asset and risk management
Configuration management
Identity and access management
Continuous monitoring and logging
Incident response
Contingency planning and recovery
involves developing and maintaining a contingency plan; assigning and training individuals for recovery operations; and executing the successful restoration of systems, assets, and capabilities

Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

7. Contingency Planning and Recovery

.

Key Practices in This Chapter

7.1 Review contingency plans: determine the extent to which the organization has arrangements for alternative processing facilities in the event that primary facilities are significantly damaged or cannot be accessed.

7.2 Assess steps taken to prevent and minimize potential damage and interruptions: determine the extent to which the organization has taken steps such as establishing an information system recovery and reconstitution capability, installing environmental controls, and providing training to ensure that staff and other system users understand their responsibilities during emergencies.

7.3 Assess testing of contingency plans: determine the extent to which the organization's contingency plans are periodically tested under conditions that simulate a disaster.

7.4 Review the documented lessons learned: determine the extent to which lessons learned from the recovery planning and processes have been incorporate into future activities.

Note: The use of "should" statements within key practices does not indicate a requirement unless explicitly stated in criteria. Auditors using this guide should apply professional judgment when determining which key practices and audit steps to implement.

Examples of Criteria to Consider

In addition to the criteria discussed in the “Identify Criteria” section of this guide, consider the following:

NIST, *Guide for Cybersecurity Event Recovery*, SP 800-184 (Gaithersburg, MD: December 2016): provides guidance to help organizations plan and prepare recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans.

NIST, *Contingency Planning Guide for Federal Information Systems,* SP 800-34, Revision 1 (Gaithersburg, MD: May 2010): provides instructions, recommendations, and considerations for government IT contingency planning.

DHS, Federal Emergency Management Agency*, Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process,* Federal Continuity Directive 2 (June 13, 2017): includes additional requirements and guidance for federal organizations when developing a business impact analysis to identify potential impacts on the performance of essential functions and the consequences of failure to sustain them.

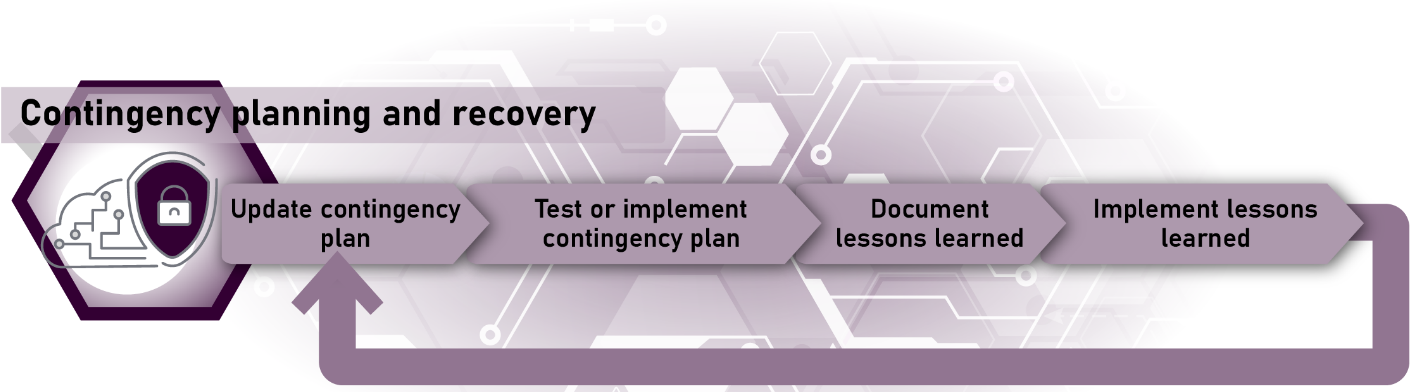
DHS, Federal Emergency Management Agency*, Federal Executive Branch National Continuity Program and Requirements,* Federal Continuity Directive 1 (January 17, 2017): establishes the framework, requirements, and processes to support the development of federal organizations’ continuity programs and specifies and defines elements of a contingency plan.

7.1 Review Contingency Plans

Contingency plans are an important part of an organization's contingency planning capability because they contain the appropriate activities to restore capabilities or services compromised by a cybersecurity event. FISMA requires each federal organization to develop, document, and implement an agency wide information security program that includes plans and procedures to ensure the continuity of operations for information systems that support the organization's operations.[112] According to NIST, conducting a business impact analysis is a key step in the contingency planning process.[113] This analysis helps identify and prioritize information systems and components critical to supporting the organization's mission and business processes. Moreover, it correlates the system with the critical mission and business processes, and based on that information, characterizes the consequences of a disruption.

According to NIST, contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency.[114] An organization's contingency plan should identify its critical systems, applications, and any subordinate or related plans. It is important that all of these plans, including the subordinate plans, be clearly documented, communicated to affected staff, and updated to reflect current operations. In addition, the organization's contingency plan should address its systems maintained by a contractor or other provider (e.g., through service-level agreements). Figure 19 summarizes the contingency planning lifecycle.

Figure 19: Contingency Planning Life Cycle


Contingency planning and recovery
Update contingency plan
Test or implement contingency plan
Document lessons learned
Implement lessons learned

Update the plan annually to account for lessons learned and changes to the information system.

Test the plan or conduct table top exercises at a frequency determined by organizational requirements.

Document the contingency plan test results and lessons learned in an after-action report.

Implement changes, such as improved training, based on lessons learned.

Source: GAO analysis of National Institute of Standards and Technology contingency planning guidance; images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

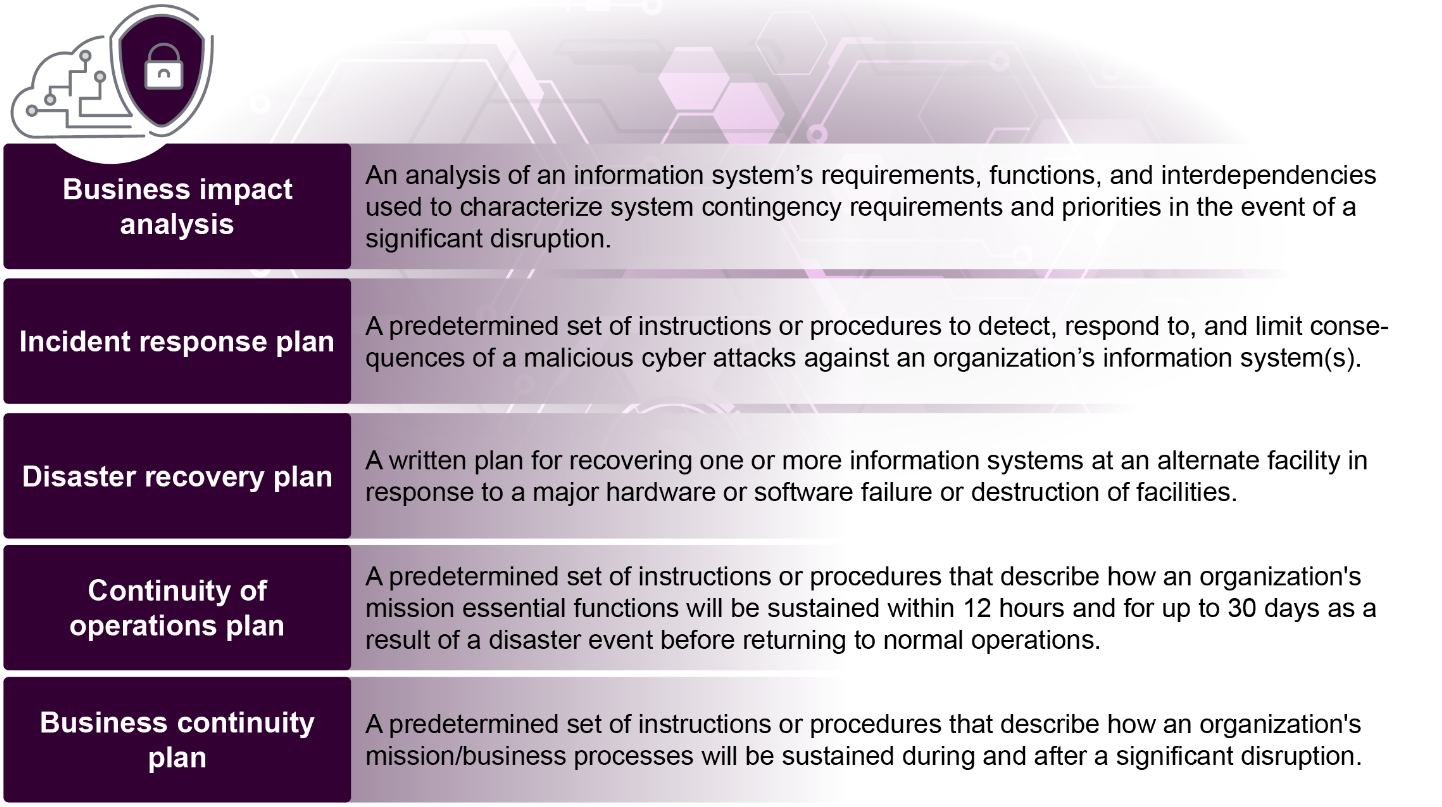
NIST 800-34, *Contingency Planning Guide for Federal Information System*s, discusses the types of contingency plans that an organization might use and how they relate to each other. Contingency plans may vary from organization to organization. NIST states that, to be effective, these plans should be maintained in a ready state that accurately reflects the system, requirements, procedures, organizational structure, and policies. Therefore, the contingency plan should be reviewed and updated regularly, or whenever significant changes occur. See figure 20 for other examples of plans related to contingency planning.

[112] 44 USC §3554(b).

[113] National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information System*s, SP 800-34, Revision 1 (Gaithersburg, MD.: May 2010).

[114] National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information System*s, SP 800-34, Revision 1 (Gaithersburg, MD.: May 2010).

Figure 20: Examples of Plans Related to Contingency Planning



Business impact analysis
An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Incident response plan
A predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s).

Disaster recovery plan
A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Continuity of operations plan
A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.

Business continuity plan
A predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Source: GAO summary of incident response plans outlined in National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, SP 800-34 Rev. 1 (Gaithersburg, MD: September 2020); images: marinashevchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

Control Objectives and Audit Procedures

Key practice 7.1 in the Chapter 7 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's contingency plans. These examples are a sample of controls and not the only controls that should be considered. Professional judgment should be used to determine which controls are appropriate for the audited organization. Additionally, these audit procedures should be considered for systems under the control of the organization. For example, these procedures may not apply to systems owned or managed by a contractor or other third-party.

7.2 Assess Steps Taken to Prevent and Minimize Potential Damage and Interruptions

Organizations should take steps to prevent or minimize the damage to automated operations that can occur from unexpected events. Documentation, such as the types of plans listed in the prior figure, help demonstrate that these steps have been taken by the organization. According to NIST, backup and recovery methods and strategies are a means to restore system operations quickly and effectively following a service disruption.[115] For example, organizations should have an information system recovery and reconstitution capability that includes routinely duplicating or backing up data files. This enables the information system to be recovered and reconstituted to its original state after a disruption or failure. As discussed in Chapter 4, organizations should also have environmental controls, such as fire suppression systems or backup power supplies, and training to ensure that staff and other system users understand their responsibilities during emergencies. Such steps,

[115] National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information System*s, SP 800-34, Revision 1 (Gaithersburg, MD.: May 2010).

especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters.

Control Objectives and Audit Procedures

Key practice 7.2 in the Chapter 7 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's steps taken to prevent and minimize potential damage and interruptions.

7.3 Assess the Testing of Contingency Plans

According to NIST, periodically testing the contingency plan validates recovery capabilities and is essential to ensure it will function as intended when activated for an emergency.[116] Testing can also reveal important weaknesses. A contingency test should address areas such as: system recovery on an alternate platform from backup media, coordination among recovery teams, internal and external connectivity, system performance using alternate equipment, restoration of normal operations, and notification procedures.[117]

Control Objectives and Audit Procedures

Key practice 7.3 in the Chapter 7 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's testing of contingency plans.

7.4 Review the Documented Lessons Learned

According to NIST, lessons learned should be identified, documented, shared, and reviewed as part of the contingency planning process.[118] Documenting lessons learned is the process of identifying and documenting experiences, knowledge, and information gained from the recovery process. The knowledge derived from sharing lessons learned serves to promote positive outcomes and reduce the possibility of negative outcomes in the future. The lessons learned process includes the processes necessary for identification, documentation, validation, and dissemination of lessons learned to appropriate personnel, and follow-up to ensure that appropriate actions were taken.

Control Objectives and Audit Procedures

Key practice 7.4 in the Chapter 7 worksheet of the supplement to this guide contains illustrative examples of controls and audit procedures to consider when auditing an organization's documented lessons learned.

[116] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[117] CISA developed tools for organizations to conduct planning exercises on a wide range of threat scenarios. See https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages for more information.

[118] National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, SP 800-34, Revision 1 (Gaithersburg, MD.: May 2010).

Appendix I: Additional Resources

Listed below is a list of example criteria and additional resources used in this guide and in the supplement to this guide. This is not an exhaustive or all-inclusive list of possible criteria. Further, the resources listed below are current as of the time of this guide's publication. Prior to using the resources below, auditors should check to make sure they are using the most current version.

General Resources

National Institute of Standards and Technology (NIST), *Assessing Security and Privacy Controls in Information Systems and Organizations*, SP 800-53A, Revision 5 (Gaithersburg, MD: January 2022): contains the assessment procedures for controls found in NIST SP 800-53.

NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Revision 5 (Gaithersburg, MD: Sept 2020): provides recommended security controls for federal information systems and organizations.

NIST, *Risk Management Framework for Information Systems and Organizations*, SP 800-37, Revision 2 (Gaithersburg, MD: December 2018): provides a structured approach to risk management and recommends managing risk based on the organization's requirements, objectives and risk tolerance level.

NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: April 2018): provides guidance for cybersecurity risk management and is composed of the framework core, the implementation tiers, and the profiles. The cybersecurity framework includes five core functions, 23 categories, and 108 subcategories.

The White House, *Executive Order on Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021): includes requirements for agencies to enhance cybersecurity and software supply chain integrity.

Office of Management and Budget (OMB), *Management's Responsibility for Internal Control*, OMB Circular No. A-123 (Washington, D.C.: December 2004): provides guidance to federal organizations on the management of internal controls. It outlines the responsibilities of federal organizations for establishing and maintaining effective internal controls over operations and assets, including requirements for conducting periodic assessments of internal controls and for addressing any identified deficiencies.

OMB, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016): establishes minimum privacy and information security requirements for federal organizations. The appendices to this circular also include responsibilities for protecting federal information resources and managing personally identifiable information (PII).

Chapter 1. General Audit Process

NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, SP 800-161, Revision 1 (Gaithersburg, MD: May 2022): provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations.

NIST, *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Gaithersburg, MD: January 2020): provides a framework to help organizations improve privacy through risk management.

NIST, National Checklist Program: provides information on a variety of security configuration checklists for specific IT products or categories of IT products.[119]

GAO, *Government Auditing Standards*, 2018 Revision, GAO-21-368G (Washington, D.C.: April 2021): known as the "Yellow Book," provides standards and guidance for auditors and audit organizations, outlining the requirements for audit reports, professional qualifications for auditors, and audit organization quality control. Auditors of federal, state, and local government programs use these standards to perform their audits and produce their reports.

GAO, *Standards for Internal Control in the Federal Government*, GAO-21-368G (Washington, D.C.: September 2014): known as the "Green Book," sets the standards for an effective internal control system for federal agencies.

Chapter 2. Asset and Risk Management

NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,* SP 800-161, Revision 1 (Gaithersburg, MD.: May 2022): provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain.

NIST, *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e* (Gaithersburg, MD: February 2022): provides guidance in accordance with the executive order that provides recommendations to federal organizations on ensuring that producers of software they procure have been following a risk-based approach for secure software development throughout the software lifecycle.

NIST, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities,* SP 800-218 (Gaithersburg, MD: February 2022): provides a core set of high-level secure software development practices that can be integrated into software development implementation to reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.

NIST, *Guide for Conducting Risk Assessments*, SP 800-30, Revision 1 (Gaithersburg, MD: September 2012): provides guidance for conducting risk assessments of federal information systems and organizations.

NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, MD: March 2011): provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems.

NIST, *Standards for Security Categorization of Federal Information and Information Systems Federal Information Processing Standards (FIPS) 199* (Gaithersburg, MD: February 2004): provides a standard for categorizing federal information and information systems according to (1) an agency's level of concern for confidentiality, integrity, and availability; and (2) the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.

NIST, *Building an Information Technology Security Awareness and Training Program,* SP 800-50 (Gaithersburg, MD: October 2003): provides guidance for building an effective IT security program and supports requirements specified in the Federal Information Security Management Act (FISMA) of 2002.

[119] https://checklists.nist.gov/.

NIST, *Information Technology Security Training Requirements: A Role and Performance-Based Model,* SP 800-16 (Gaithersburg, MD: April 1998): provides a framework for IT security training.

Department of Homeland Security (DHS), *Securing High Value Assets,* BOD 18-02 (May 7, 2018): contains requirements for federal organizations to take specific actions to protect their most critical systems.

OMB, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, M-22-18 (Washington, D.C.: Sept. 14, 2022): requires each federal agency to comply with the NIST guidance when using third-party software on the agency's information systems or otherwise affecting the agency's information.

Chapter 3. Configuration Management

NIST, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology,* SP 800-40, Revision 4 (Gaithersburg, MD: April 2022): includes guidelines to help organizations improve their enterprise patch management planning so that they can strengthen their management of risk.

NIST*, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers,* SP 800-70, Revision 4 (Gaithersburg, MD: February 2018): explains how to use the National Checklist Program checklists and describes the policies, procedures, and general requirements for participation in the program.

NIST*, Guide for Security-Focused Configuration Management of Information Systems,* SP 800-128 (Washington, D.C.: August 2011): provides guidelines for organizations responsible for managing and administering the security of federal information systems and associated environments of operation.

NIST, *Minimum Security Requirements for Federal Information and Information Systems,* FIPS 200 (Washington, D.C.: March 2006): specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements.

DHS, *Improving Asset Visibility and Vulnerability Detection on Federal Networks,* BOD 23-01 (Oct. 3, 2022): contains requirements and implementation guidance on asset discovery and vulnerability enumeration which are essential for improving operational visibility for a successful cybersecurity program.

DHS, *Vulnerability Remediation Requirements for Internet-Accessible Systems,* BOD 19-02 (Apr. 19, 2019): establishes requirements for federal organizations to review and remediate critical vulnerabilities on Internet-facing systems.

OMB, *Memorandum for Heads of Executive Departments and Agencies: Completing the Transition to Internet Protocol Version 6 (IPv6),* M-21-07 (Washington, D.C.: November 2020): provides guidance on the federal government's operational deployment and use of IPv6 and includes specific steps federal organizations are expected to take to complete the transition.

Defense Information Systems Agency (DISA) security technical implementation guides (STIGS): provides an additional source of configuration guidance for network devices, software, databases and operating systems.

Chapter 4. Identity and Access Management

NIST*, Personal Identity Verification (PIV) of Federal Employees and Contractors,* FIPS 201-3 (Gaithersburg, MD: January 2022): establishes a standard for a personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive (HSPD)-12.

NIST*, Resilient Interdomain Traffic Exchange: Border Gateway Protocol (BGP) Security and Denial of Service (DDoS) Mitigation*, SP 800-189 (Gaithersburg, MD: December 2019): provides guidelines and recommendations for deploying protocols that improve the security of interdomain traffic exchange.

NIST*, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* – SP 800-60 *Revision 1* (Gaithersburg, MD: August 2008): contains the basic guidelines for mapping types of information and information systems to security categories.

OMB, *Memorandum for Heads of Executive Departments and Agencies: Update to the Trust Internet Connections (TIC) Initiative,* M-19-26 (Washington, D.C.: September 2019): provides an approach for federal organizations to implement the Trust Internet Connections initiative with increased flexibility to use modern security capabilities.

OMB, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, M-19-17 (Washington, D.C.: May 21, 2019): provides policy-level guidance for federal organizations to identify, credential, monitor, and manage user access to information and information systems and adopt sound processes for authentication and access control.

OMB*, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: September 26, 2003): directs federal organizations to conduct reviews of how information about individuals is handled within their agencies when they use IT to collect new information, or when organizations develop or buy new IT systems to handle collection of PII.

DHS, Homeland Security Presidential Directive (HSPD), *Policy for a Common Identification Standard for Federal Employees and Contractors,* HSPD-12 (Jan. 27, 2022): mandates a federal standard for secure and reliable forms of identification.

Chapter 5. Continuous Monitoring and Logging

NIST, *Automation Support for Security Control Assessments: Volume 1: Overview, NISTIR 8011 Volume 1* (Gaithersburg, MD: June 2017): introduces concepts to support automated assessment of most of the security controls in NIST SP 800-53.

NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* SP 800-137 (Gaithersburg, MD: September 2011): provides guidelines to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program.

NIST, *Guide to Computer Security Log Management*, SP 800-92 (Gaithersburg, MD: September 2006): provides guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise.

OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents,* M-21-31(Washington, D.C.: August 27, 2021): addresses the requirements in section 8 of Executive Order 140828 for logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center of each agency.

Chapter 6. Incident Response

NIST*, Guide to Malware Incident Prevention and Handling for Desktops and Laptops,* SP 800-83, Revision 1 (Gaithersburg, MD: July 2013): provides recommendations for improving an organization's malware incident prevention measures and for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents.

NIST, *Computer Security Incident Handling Guide*, SP 800-61, Revision 2 (Gaithersburg, MD: August 2012): provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

OMB, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirement*, M-23-03 (Washington, D.C.: December 2022): provides updated reporting guidance in accordance with FISMA and Executive Order 14028.

OMB, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12 (Washington, D.C.: January 2017): sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals.

CISA, *Cybersecurity Incident & Vulnerability Response Playbooks* (Washington, D.C.: November 2021): provides operational procedures for planning and conducting cybersecurity incident and vulnerability response activities in federal civilian executive branch agencies, including the collection and preservation of data for incident verification, categorization, prioritization, mitigation, reporting, and attribution.

Chapter 7. Contingency Planning

NIST, *Guide for Cybersecurity Event Recovery*, SP 800-184 (Gaithersburg, MD: December, 2016): provides guidance to help organizations plan and prepare recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans.

NIST, *Contingency Planning Guide for Federal Information Systems,* SP 800-34, Revision 1 (Gaithersburg, MD: May 2010): provides instructions, recommendations, and considerations for government IT contingency planning.

DHS, Federal Emergency Management Agency, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process,* Federal Continuity Directive 2 (June 13, 2017): includes additional requirements and guidance for federal organizations when developing a business impact analysis to identify potential impacts on the performance of essential functions and the consequences of failure to sustain them.

DHS, Federal Emergency Management Agency, *Federal Executive Branch National Continuity Program and Requirements,* Federal Continuity Directive 1 (Jan. 17, 2017): establishes the framework, requirements, and processes to support the development of federal organizations' continuity programs and specifies and defines elements of a contingency plan.

Appendix II: Glossary

Baseline configuration. A set of specifications for a system, or configuration item within a system that has been formally reviewed and agreed on at a given point in time and which can be changed only through change control procedures. The baseline configuration is used for future builds, releases, and/or changes.

Business continuity plan. The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Business impact analysis. An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Computer Security Incident Response Team. A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a computer incident response team, a computer incident response center, or a computer incident response capability.

Continuous monitoring. A method of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Cybersecurity control. A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Cybersecurity and Infrastructure Security Agency (CISA). An operational component agency within the Department of Homeland Security (DHS) with the responsibility to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructures in the face of both physical and cyber threats.

Federal Information Security Modernization Act (FISMA). FISMA, and its predecessor, the Federal Information Security Management Act of 2002, established a framework for standards by defining roles and responsibilities for OMB, DHS, NIST, and federal agencies. The law requires agencies submit regular inventories of their major information systems to OMB and that they report annually on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise.

Firewall. A system design to prevent unauthorized access to or from a private network. A firewall is often used to prevent internet users from accessing private networks connected to the internet.

Incident response. The mitigation of violations of security policies and recommended practices.

Intrusion detection system (IDS). A system or software that monitors and analyzes network or system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

NIST Cybersecurity Framework. The framework provides guidance for cybersecurity risk management and is composed of the framework core, the implementation tiers, and the profiles. The framework includes five core functions, 23 categories, and 108 subcategories.

Patch management. The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Plan of action and milestones (POA&M). A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for meeting the tasks, and scheduled milestone completion dates.

Security awareness. A program that explains proper rules of behavior for the use of agency information systems and information. The program communicates IT security policies and procedures that need to be followed.

Spam. Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Technical controls. The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Voice over Internet Protocol. A term used to describe the transmission of packetized voice using the internet protocol (IP) and consists of both signaling and media protocols.

Vulnerability scanning. A technique used to identify hosts/host attributes and associated vulnerabilities.

Appendix III: Working Group Participants

Listed below are the participants from the working group we held in April 2021. Their titles and organizations are current as of that time.

Cynthia Agloro, Grant Thornton, Senior Manager

Larry Akinkuotu, Department of Housing and Urban Development, OIG, IT Specialist

Dan Altobelli, New Jersey State Auditor, Manager

Brett Baker, U.S. Nuclear Regulatory Commission, Assistant Inspector General for Audit

Baback Bazri, Ernst & Young, Principal, Advisory Services

Bob Broda, North Carolina State Auditor, Advisor Compliancy

Kelli Brown-Barnes, U.S. Securities and Exchange Commission, OIG, Audit Manager

Daniel Burrows, U.S. Consumer Product Safety Commission, IT Auditor

Douglas Carney, formerly at U.S. Securities and Exchange Commission, OIG, Auditor

Miki Cestnik, Montana Legislative Audit Division, IS Audit Manager

Erin Cole, U.S. Department of Energy, OIG, Director, Technology

Angel Contreras, Castro & Company, LLC, Principal

Thomas Elchenko, OPM, Senior Team Leader, IS Audit Group

Kelly Fahel, Grant Thornton, Senior Manager

George Fallon, RMA Associates, IT Audit Lead

Teresa Furnish, Secretary of State, Oregon Audits Division, IT Audit Manager

Jonathan Giguere, Ernst & Young, Senior Manager

Peter Gross, North Carolina State Auditor, Audit Supervisor

Tyler Harding, Amazon, AWS Security and DOD Compliance Program Manager

Marc Hebert, RMA Associates, Director

Stu Henderson, The Henderson Group, Mainframe Specialist for IPA Firms

Eric W. Keehan, Office of Personnel Management OIG, Group Chief

Babur Kohy, Director of Academics at ISACA GWDC

Janet Knauff, U.S. Railroad Retirement Board, OIG, Supervisory Auditor

Phyllis Lee, Center for Internet Security (CIS), Senior Director for Controls

Wayne Liu, RMA Associates, IT Director

Leon Lucas, Department of Transportation, OIG, Program Director

Reza Mahbod, RMA Associates, President

Bobbi Markley, Department of Defense, OIG

Scott Marler, Tennessee Valley Authority, OIG, IT Audit Manager

Olga Mason, U.S. Social Security Administration, OIG, Acting Audit Manager

Mark Mathison, Minnesota Office of the Legislative Auditor, IT Audit Director

Peter Miller, North Carolina State Auditor, Information Systems Audit Supervisor

Sarah Mirzakhani, Clifton Larson Allen, LLP, IT Principal

Jamila Moore, U.S. Small Business Administration, OIG, IT Specialist

Phillip Moore, Kearney & Company, Partner, IT Audit Practice Leader

Kirsten Orr, Grant Thornton, IT Audit Senior Manager

Victoria Pillitteri, National Institute of Standards and Technology, Cybersecurity Engineer

Laura A. Rainey, National Science Foundation, OIG, Director of Financial & IT Audits

Larry Sanes, Department of Justice, OIG, IT Specialist

Melissa Schuiling, Michigan State Auditor, Division Administrator over IT Audits
Loren Schwartz, Cotton & Company, Partner
Liping Tan, Defense Intelligence Agency, OIG
Jose Torres, ISACA, Director of Programs
Rathini Vijayaverl, NIST, Office of IS Management
Vernon Utley, North Carolina State Auditor, Director, Information Systems Audit
Kristen Welch, Ernst & Young, Senior Manager
Ko Williams, Health and Human Services, OIG, Cybersecurity & IT Audit Division
Yin Yin Hon, Commonwealth of Massachusetts State Auditor's Office, IT Audit Supervisor

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342, MarinosN@gao.gov

Vijay A. D’Souza, (202) 512-7650, DsouzaV@gao.gov

Jennifer R. Franks, (404) 679-1831, FranksJ@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Rosanna Guerrero and Tammi Kalugdan (assistant directors), Tina Torabi (analyst in charge), Edward Alexander Jr., Logan Arkema, Sher’rie Bacon, Lauri Barnes, Tracey Bass, Brottie Barlow, Season Burris, Chris Businsky, Garret Chan, Larry Crosland, Kristi Dorsey, Stephen Duraiswamy, Wayne Emilien, Corey Evans, Becca Eyler, Adella Francis, Charles Hubbard III, George Kovachick, Ahsan Nasar, Duc Ngo, Brandon Sanders, Priscilla Smith, Andrew Stavisky, Daniel Swartz, Walter Vance, Adam Vodraska, Marshall Williams Jr., and Alec Yohn. We also acknowledge the contributions of many individuals in GAO’s Information Technology and Cybersecurity team who dedicated time and expertise to developing and improving this guide.