

GAO's Cybersecurity Program Audit Guide (GAO-23-104705)

www.gao.gov/cbaa

Vijay A D'Souza and West Coile

U.S. Government Accountability Office

Information Technology & Cybersecurity
Team

October 24, 2024

Agenda

- **About GAO**
- **Cybersecurity Challenges**
- **GAO's Cybersecurity-Related Work**
- **Cybersecurity Program Audit Guide**
- **Who Uses CPAG**
- **Feedback**
- **Q& A**

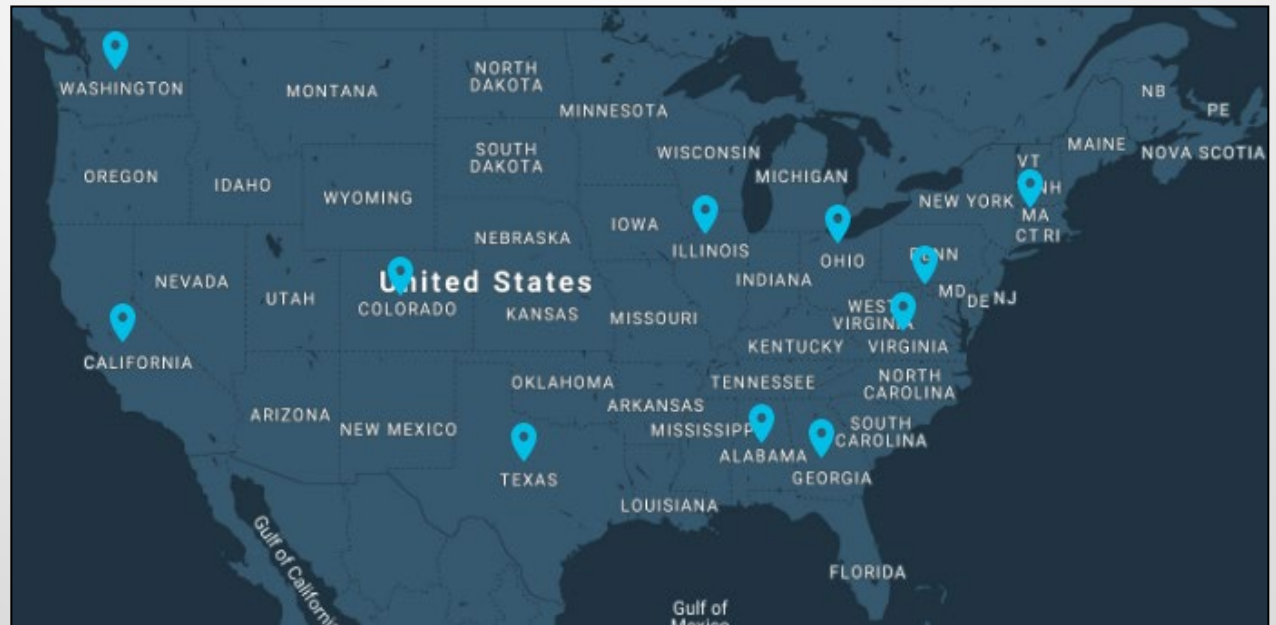
GAO



Source: GAO image



Source: GAO image



Source: GAO image

Cybersecurity Challenges

Four major cybersecurity challenge areas

<p>Establishing a comprehensive cybersecurity strategy and performing effective oversight</p>	<p>Securing federal systems and information</p>	<p>Protecting cyber critical infrastructure</p>	<p>Protecting privacy and sensitive data</p>
<p>1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.</p>	<p>5 Improve implementation of government-wide cybersecurity initiatives.</p>	<p>8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).</p>	<p>9 Improve federal efforts to protect privacy and sensitive data.</p>
<p>2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).</p>	<p>6 Address weaknesses in federal agency information security programs.</p>		
<p>3 Address cybersecurity workforce management challenges.</p>	<p>7 Enhance the federal response to cyber incidents.</p>		
<p>4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).</p>			<p>10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.</p>

Information technology & Cybersecurity (ITC)

The vision of the ITC Team (approximately 200 people) is to provide Congress with nonpartisan and independent insight into federal efforts to

- effectively and securely manage information technology,
- ensure the cybersecurity of the nation, and
- effectively manage the collection, dissemination and quality of government information.



Information technology & Cybersecurity (ITC)

The ITC team oversees federal efforts to

- improve IT management practices,
- ensure the efficiency of IT acquisitions and operations,
- adopt IT management best practices,
- protect information systems, and
- improve how the government protects individual privacy and sensitive data.

GAO's Cybersecurity Work



Source: Microsoft stock image

High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation

[GAO-24-107231](#)

Published: Jun 13, 2024



Source: Microsoft stock image

NASA Cybersecurity: Plan Needed to Update Spacecraft Acquisition Policies and Standards

[GAO-24-106624](#)

Published May 01, 2024



Source: Microsoft stock image

Artificial Intelligence: Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity

[GAO-24-106246](#)

Published: Feb 07, 2024

Poll Question

What is your level of cybersecurity experience?

- a) Not much/beginner
- b) I know enough to be dangerous (but I'm not)
- c) Some might say I'm an expert

Poll Question

What is your primary job focus in cybersecurity?

- a) Develop/implement controls
- b) Test/evaluate controls
- c) Incident response
- d) Policy/management

Cybersecurity Program Audit Guide

**GAO issued a new cybersecurity
program audit guide for conducting
cybersecurity performance audits.**

(GAO-23-104705)

**Asset and risk
management**



**Configuration
management**



**Identity
and access
management**



**Continuous
monitoring
and logging**



**Incident
response**

**Contingency
planning and
recovery**



Overview of the Cybersecurity Program Audit Guide (CPAG)

- Provides a set of methodologies and audit procedures to evaluate components of agency cybersecurity programs and systems.
- Relies on practices covered by the National Institute of Standards and Technology (NIST) guidance, Office of Management and Budget (OMB), and industry leading practices.



CPAG Impact

- 1. Enhanced security posture:** Implementing a robust cybersecurity audit guide can contribute to an enhanced security posture. By regularly identifying vulnerabilities, agencies can proactively strengthen their defenses against cyber threats.
- 2. Protecting sensitive data:** Having a sound cybersecurity audit guide helps in safeguarding sensitive data. Through comprehensive assessments, agencies can identify and address potential problems early to ensure the confidentiality, integrity, and availability of critical information.
- 3. Regulatory compliance:** Adhering to a well-defined cybersecurity audit methodology ensures compliance with regulatory requirements.
- 4. Cybersecurity awareness and culture:** Implementing a cybersecurity audit methodology fosters a culture of awareness within the organization. Employees who are more conscious of security practices can help to maintain a secure environment.

CPAG Features



Points to many different criteria in the NIST Cybersecurity Framework and NIST 800-53 Rev. 5 controls, as well as others

Provides information on how to conduct a cybersecurity audit

Provides suggested audit steps

Differences with the Federal Information System Controls Audit Manual (FISCAM)

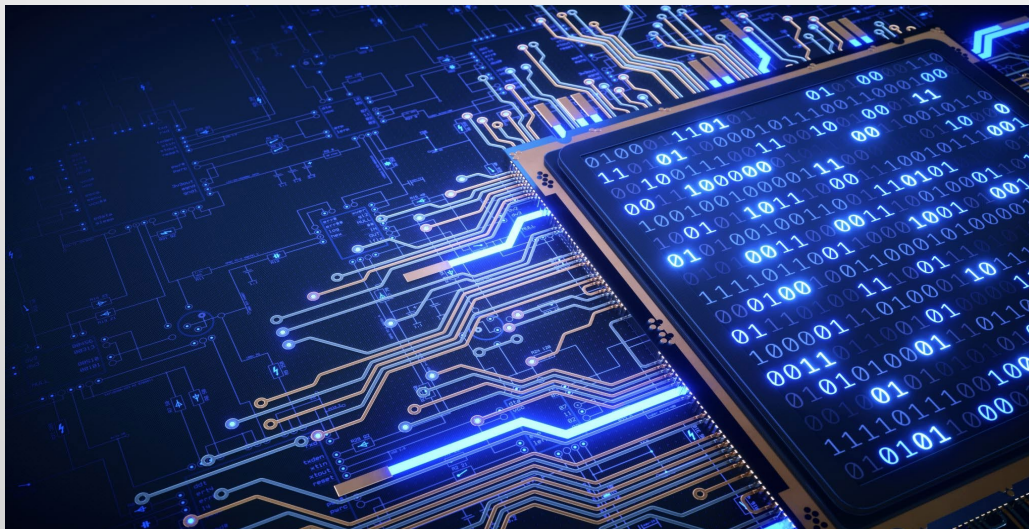
- FISCAM provides a methodology for assessing information system controls related to financial audits or attestation engagements.
- FISCAM was issued in 1999 and updated in 2009. An exposure draft of FISCAM was issued in June 2023 (GAO-23-104975) and FISCAM 2024 (GAO-24-107026) was issued September 5, 2024.
- This new revision reorders FISCAM to follow GAO's Financial Audit Manual, as many of the reviewed controls remain relevant to financial audits.

Development of CPAG

- Issued an initial questionnaire to the existing FISCAM users and asked for input on possible improvements. The users included federal Offices of Inspectors General, independent public accounting firms, and state auditors.
- Held 10 focus groups with internal and external stakeholders. The focus groups included senior executives, IT managers, and analysts across GAO; federal Inspectors General; independent public accounting representatives; and state auditors.
- Interviewed officials from NIST, the Center for Internet Security, and ISACA (Information Systems Audit and Control Association), among others for their input and comments.
- Performed content analysis of focus group responses to identify most frequently suggested changes.

CPAG Structure

- Organized into seven chapters with accompanying supplements
- Not intended to list every possible control objective and audit procedure



Source: Microsoft stock image

CPAG Structure

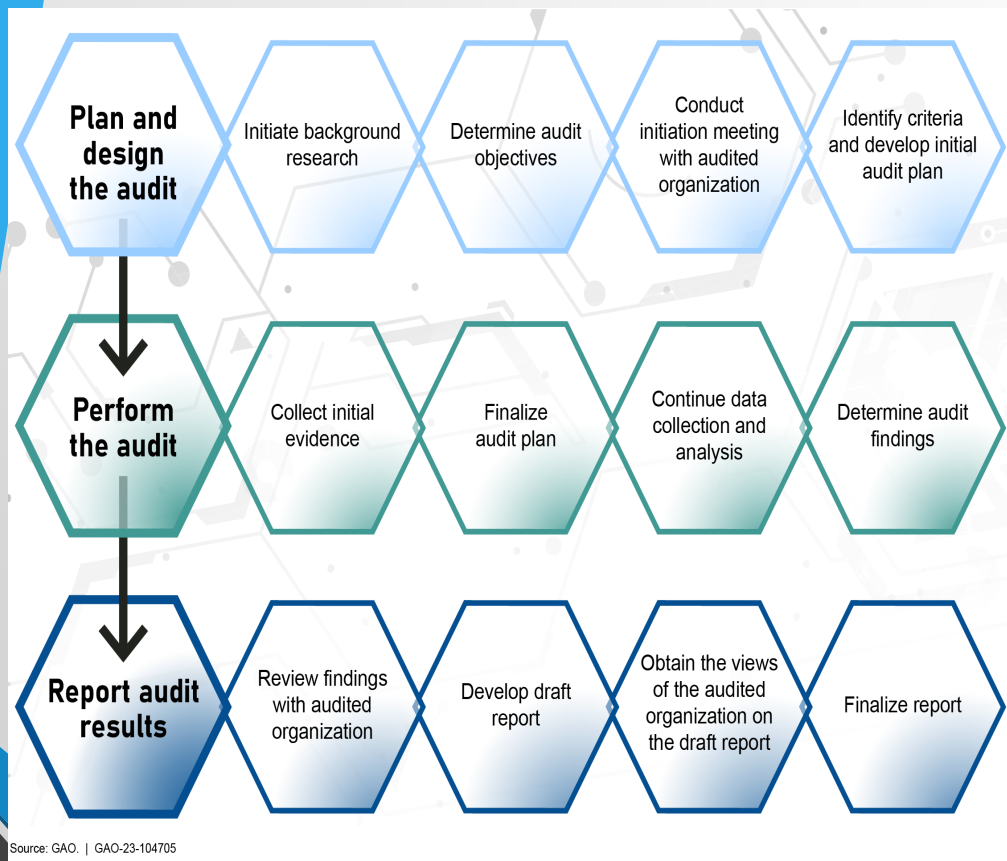
Chapter 1: general guide to the audit process

Chapters 2-7: details on the main components of a comprehensive cybersecurity audit

Appendixes: glossary and a suggested list of criteria to use

Supplement attachment: Suggested audit procedure steps (Excel spreadsheets)

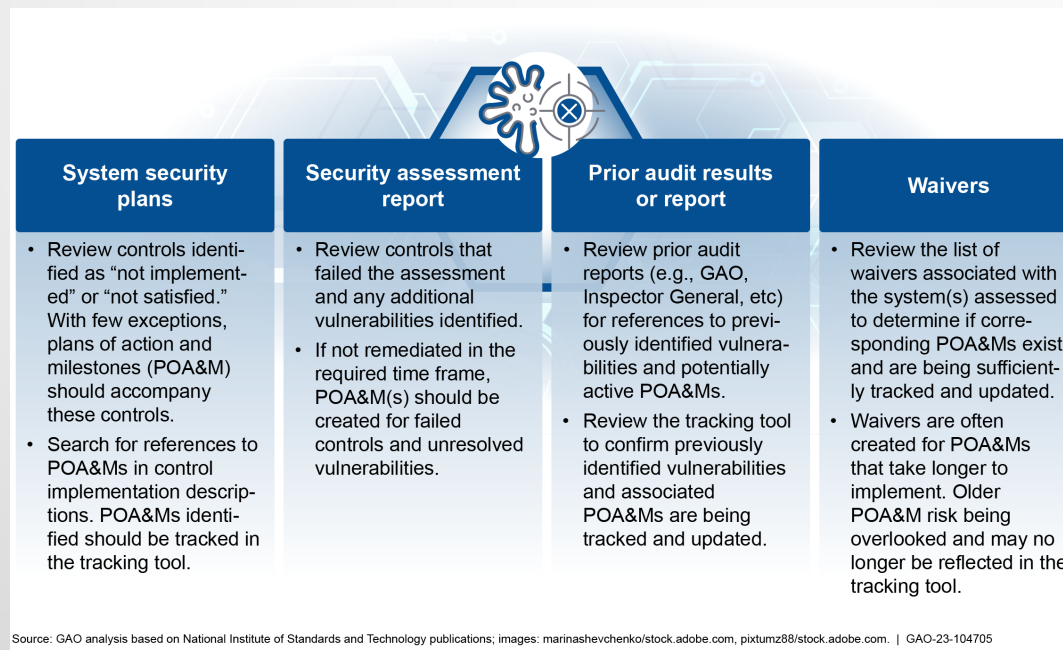
Chapter 1: Cybersecurity Program Audit Process



- CPAG is based on generally accepted government auditing standards and systemic processes that GAO uses for performance audits.
- This chapter is a general guide to the audit process and the main phases of a cybersecurity performance audit:
 - 1.1 Planning and designing
 - 1.2 Performing
 - 1.3 Reporting

Chapter 1: How to Use CPAG

- Determine your audit scope and boundaries: **You can choose which chapter(s) of the CPAG to focus on after you have determined the audit's scope**
 - For example: CPAG discusses which documents to review when assessing plans of action and milestones:



System security plans	Security assessment report	Prior audit results or report	Waivers
<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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: marinashchenko/stock.adobe.com, pixtumz88/stock.adobe.com. | GAO-23-104705

- Prioritize key assets of interest—the criteria used to prioritize the systems should reflect the audit objectives.

Chapter 1: How to Use CPAG *(Continued)*

- Develop audit initial plan
- Develop audit procedures—CPAG 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
- Collect data and conduct analysis of documentation
- Finalize audit plan and perform audit

Chapters 2 to 7: Components



- Security management practices of reviewing policies and procedures are embedded in each of the six main components.
- Each chapter contains key practices and criteria covered by NIST guidance, OMB policies and guidance, as well as industry leading practices, plus a corresponding supplement Excel sheet attachment with illustrative examples of controls, audit procedures, and criteria.

Criteria Used in CPAG

Examples of criteria and standards generally relevant to cybersecurity audits of federal agencies include:

- FISMA requirements,
- NIST risk management framework,
- NIST SP 800-53 revision 5,
- NIST Cybersecurity Framework version 1.1,¹
- OMB guidance, and
- DHS binding operational directives.

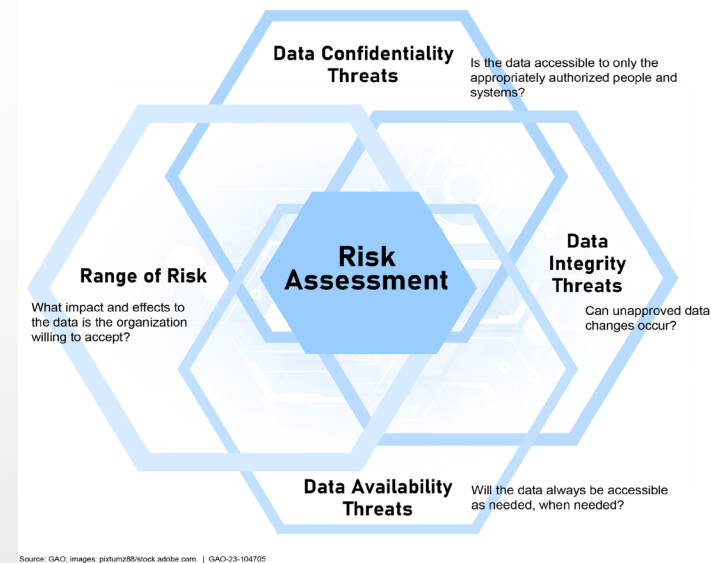
¹NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Gaithersburg, MD: April 2018). NIST released a new version in February 2024 call the NIST Cybersecurity Framework (CSF) Version 2.0 (Gaithersburg, MD: February 2024).



Question: What criteria do you use
for audit/evaluation?

Chapter 2: Asset and Risk Management

- Involves developing an organizational understanding of the risks to assets, systems, information, and operational capabilities.
- Key practices:
 - 2.1 Assess IT governance
 - 2.2 Assess management of assets
 - 2.3 Assess risk management strategy
 - 2.4 Review risk assessment
 - 2.5 Review plans of actions and milestones
 - 2.6 Assess management of supply chain risk
 - 2.7 Evaluate security awareness and training program



Chapter 2: Asset and Risk Management – Supplement Example

Control Objectives	Audit Procedures	Examples of Control Criteria
2.1.2 Determine whether policies and procedures are implemented as intended.	<ol style="list-style-type: none"> 1. Review security policies and procedures to ensure they include elements such as legal and regulatory requirements. 2. Interview management personnel with information security and privacy responsibilities to determine whether policies and procedures are implemented as intended. 3. For selected policies and procedures, determine the extent to which they are periodically tested for compliance and assess their enforcement. 	<p>National Institute of Standards and Technology (NIST) SP 800-53 Revision 5: Risk Assessment (RA) RA-1 Policy and Procedures</p> <p>NIST Cybersecurity Framework Version 1.1: ID.GV-1 (Identify Governance): Organizational cybersecurity policy is established and communicated. ID.RA-1 (Identify Risk Assessment): Asset vulnerabilities are identified and documented. ID.RM-1 (Identify Risk Management Strategy): Risk management processes are established, managed, and agreed to by organizational stakeholders.</p> <p>NIST SP 800-30 Revision 1 NIST SP 800-37 Revision 2 NIST SP 800-100</p>

How to Apply Chapter 2 to Audits:

- **For example:** The objective is to review an agency's implementation of its IT security policies.
- **Consult CPAG and find control objective 2.1.2:** Determine whether policies and procedures are implemented as intended.
- **Follow the Audit Procedures listed in the CPAG workbook**
- **Sample Finding:** The policies and procedures are properly documented and approved by relevant management. However, the agency fails to periodically test its policies or procedures, leading to inconsistent implementation of security practices. This puts the agency at greater risk of cybersecurity incidents.
- **Sample Recommendation:** Periodically test security polices and procedures.

Chapter 3: Configuration Management

- Involves the identification and management of security features for an information system's hardware, software, and firmware and systematically controlling changes to its configuration.
- Key practices:
 - 3.1 Review configuration management policies, plans, and procedures
 - 3.2 Review current configuration identification information
 - 3.3 Assess management of configuration changes
 - 3.4 Assess configuration monitoring activities
 - 3.5 Assess software update process
 - 3.6 Review documentation of emergency configuration changes



How to Apply Chapter 3 to Audits:

- **For example:** The objective is to assess the accuracy of an agency's system inventory.
- **Consult CPAG and find control objective 3.2.1:** Determine if a current and comprehensive baseline inventory of hardware, software, and firmware is documented, complete, and accurate.
- **Follow the Audit Procedures listed in the CPAG workbook**
- **Sample Finding:** A number of information systems are not documented in the agency's system inventory. As a result, these systems are not regularly monitored and do not meet the agency's configuration requirements.
- **Sample Recommendation:** Ensure the agency documents a current, complete and comprehensive baseline inventory of hardware, software, and firmware.

Chapter 4: Identity & Access Management

- Involves limiting or detecting inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, & disclosure



Source: Microsoft stock image

- **Key practices:**

- 4.1 Evaluate system boundary protection
- 4.2 Assess identification and authentication mechanisms
 - 4.2.1 Assess logical access controls
 - 4.2.2 Assess physical access controls
- 4.3 Assess data protection and privacy activities
- 4.4 Review the security policies on hiring, transfer, termination, and performance

How to Apply Chapter 4 to Audits:

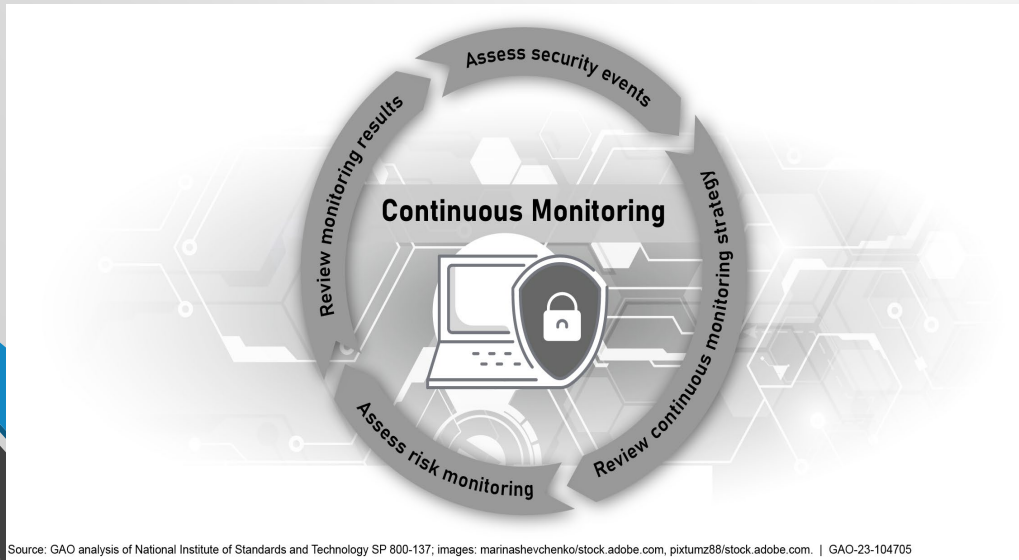
- **For example:** The objective is to test the agency's network.
- **Consult the CPAG workbook and find control objective 4.1.2:** Determine if networks are appropriately configured to adequately protect access paths within and between systems and using appropriate technological controls (e.g., routers and firewalls)
- **Follow the Audit Procedures listed in the CPAG workbook**
- **Sample Finding:** A particular user ID doesn't have full access rights (read, write, execute), but it has limited access rights (read-only). However, this user ID can view sensitive files and edit the data.
- **Sample Recommendation:** Ensure users have appropriate access rights.

Chapter 5: Continuous Monitoring & Logging

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

Key practices:

- 5.1 Assess Continuous Monitoring
- 5.2 Review the Continuous Monitoring Strategy and Implementation
- 5.3 Review Security Control Assessments and Assessor Independence
- 5.4 Review Automated Monitoring Results
- 5.5 Assess Security Event Identification, Logging, and Retention



How to Apply Chapter 5 to Audits:

- **For example:** The objective is to determine if service provider connections are secured and monitored.
- This relates to **CPAG Control Objective 5.5.5:** Assess whether service provider connections are secured and monitored.
- **Follow the Audit Procedures listed in the CPAG workbook**
- **Sample Finding:** The agency has standards and procedures to monitor service provider activity. The agency also has contracts and service legal agreements for the external service providers in place. However, the agency did not test the service provider connections for compliance with applicable standards.
- **Sample Recommendation:** Ensure that service provide connections are tested for compliance with applicable standards.

Chapter 6: Incident Response

- Involves developing and implementing actions to take when actual or potential jeopardy to the confidentiality, integrity, or availability of an information system is identified



Source: Microsoft stock image

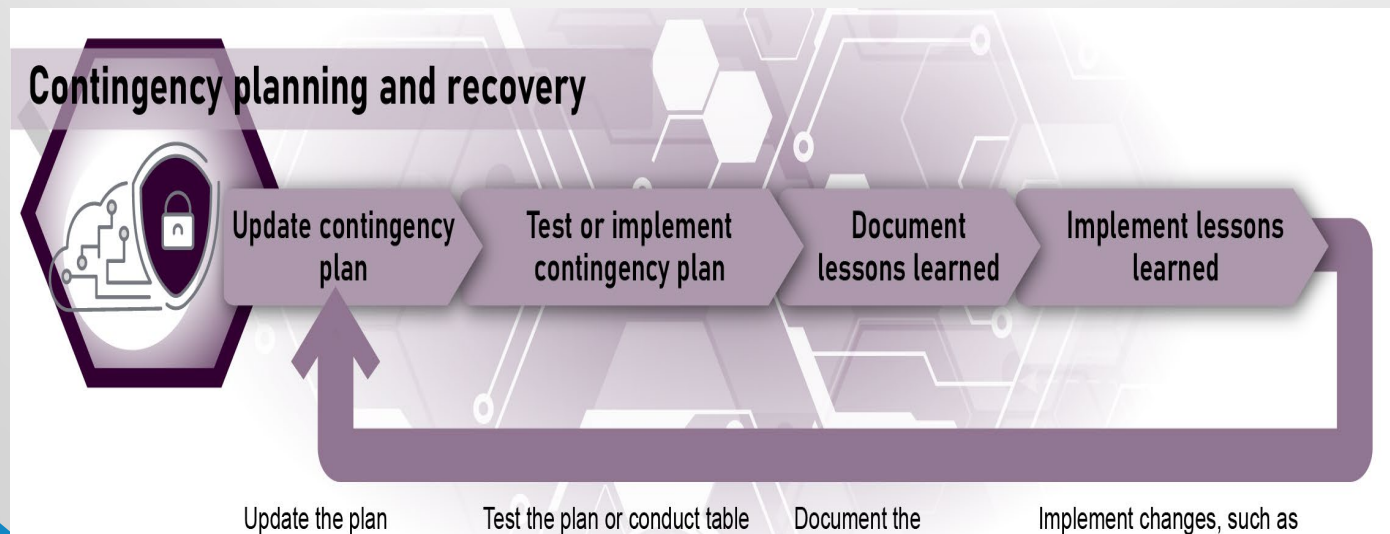
- **Key practices:**
 - 6.1 Assess Incident Response Policies, Plans, and Procedures
 - 6.2 Assess Incident Response Capabilities
 - 6.3 Assess Incident Response Training and Testing Capabilities
 - 6.4 Assess Incident Monitoring Capabilities

How to Apply Chapter 6 to Audits:

- **For example:** The objective is to assess an agency's incident response testing and training capabilities.
- This relates to the following **CPAG Control Objectives:**
 - **6.3.1:** Determine if the organization conducts incident response training according to policy, plans, procedures, and best practices.
 - **6.3.2:** Determine if the organization performs periodic incident response testing according to policy, plans, and best practices.
- **Follow the Audit Procedures listed in the CPAG workbook**
- **Sample Finding:** Agency personnel are required to report suspected security incidents and, per sampled training records, have completed required trainings. Additionally, the agency tests responses to data breaches, although it does not specifically test for ransomware incidents.
- **Sample recommendation:** Ensure the agency performs periodic incident response testing to include ransomware incidents.

Chapter 7: 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
- **Key practices:**
 - 7.1 Review Contingency Plans
 - 7.2 Assess Steps Taken to Prevent and Minimize Potential Damage and Interruptions
 - 7.3 Assess Testing of Contingency Plans
 - 7.4 Review the Documented Lessons Learned

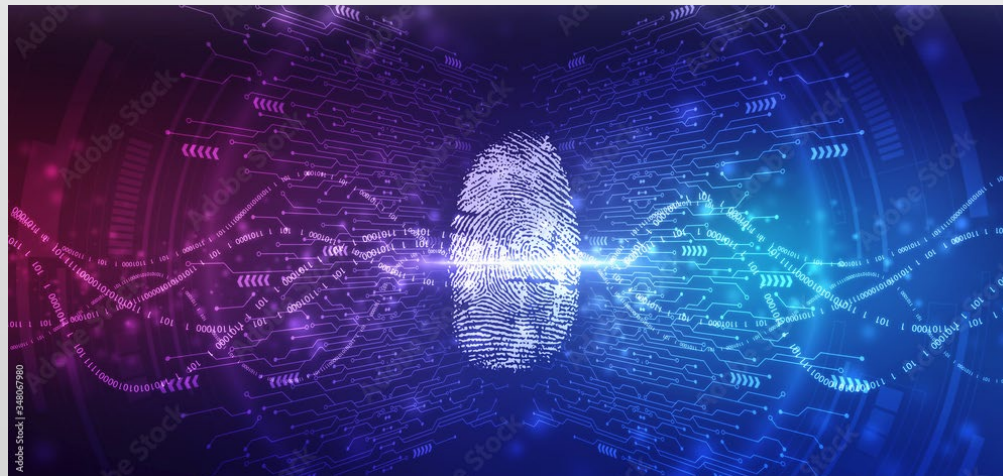


How to Apply Chapter 7 to Audits:

- **For example:** The objective is to assess an agency's testing of its contingency plans.
- This relates to **CPAG Control Objective 7.3.1:** Determine if contingency plans are periodically tested under conditions that simulate a disaster and whether the frequency of testing is in accordance with organizational requirements.
- **Follow the Audit Procedures listed in the CPAG workbook**
- **Sample Finding:** The agency has testing policies and methodologies which appropriately address selected disaster scenarios. Additionally, the agency tests its contingency plans on a routine basis. However, the agency's contingency plan test results do not meet department-wide recovery time requirements.
- **Sample recommendation:** Identify the specific reasons why the contingency plan failed to meet the recovery time requirements. This could involve analyzing the performance of critical systems, the efficiency of recovery processes, resource availability, and coordination among teams.

CPAG Use in GAO Cyber Audits: National Background Investigation Services (NBIS)

- **Objective:** Assess the extent that the Defense Counterintelligence and Security Agency (DCSA) has implemented cybersecurity controls for selected NBIS systems and legacy background investigation systems
- We are assessing the Configuration Management (**Chapter 3**), Identity & Access Management (**Chapter 4**), and Continuous Monitoring and Logging (**Chapter 5**) of selected NBIS systems.



Source: Microsoft stock image

CPAG Use in the State of Florida Office of the Inspector General (OIG)

- The State of Florida OIG used the CPAG planning/preliminary survey section as a guide for its enterprise cybersecurity audits.
- It used the CPAG for its enterprise audit topics in formulating its audit program for Security Continuous Monitoring, Identity and Access Management, Incident Response, and Asset Management.
- The Chief IG stated the “CPAG cyber guidance is a readily available tool for us to periodically benchmark our overall cyber auditing activities across the enterprise.”

Poll Question

Which emerging technology do you believe will have the most significant impact on cybersecurity auditing in the near future?

- a) Artificial Intelligence and Machine Learning
- b) Quantum Computing
- c) Internet of Things (IoT)
- d) 5G Networks
- e) Zero Trust Architecture

Have Feedback?

- We plan to have revisions and updates for the CPAG in the near future.
- Do you have any ideas on what else we should include?

Team's mailbox:
CPAG@gao.gov

- **Vijay A. D'Souza, DsouzaV@gao.gov, Director**
- **Jennifer R. Franks, FranksJ@gao.gov, Director**
- **Tammi Kalugdan, KalugdanT@gao.gov, Assistant Director**

Q & A

GAO Contacts

GAO on the web

Web site: <https://www.gao.gov/>

Congressional Relations

Nikki Clowers, Managing Director, ClowersA@gao.gov
(202) 512-4010, U.S. Government Accountability Office
441 G Street, NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Managing Director, kaczmarekS@gao.gov,
(202) 512-8590, U.S. Government Accountability Office
441 G Street, NW, Room 7149, Washington, DC 20548

Copyright

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.