



GAO'S CYBERSECURITY PROGRAM AUDIT GUIDE (GAO-23-104705)

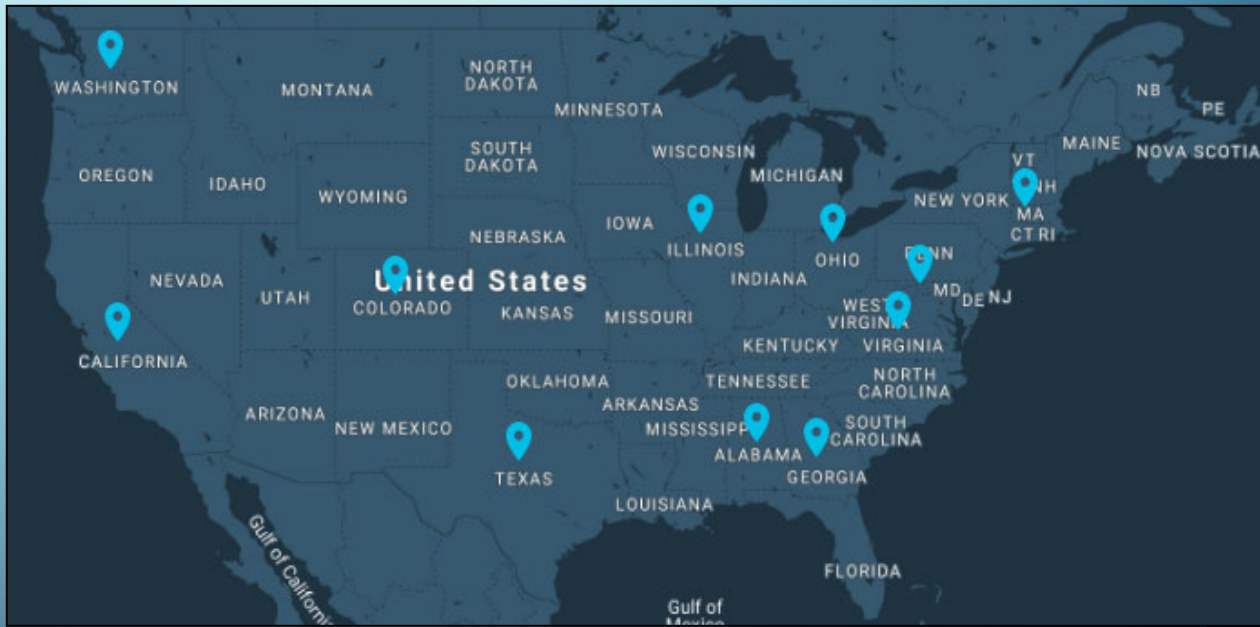
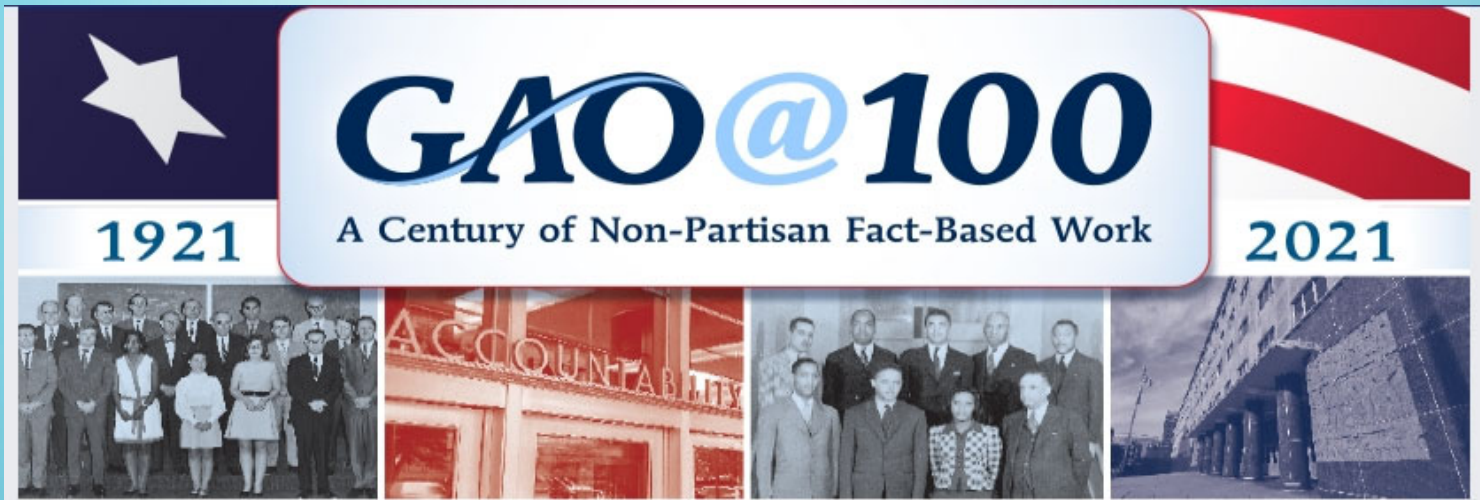
WWW.GAO.GOV/CPAG

**Vijay D'Souza and Jennifer Franks
U.S. Government Accountability Office
Directors, Information Technology &
Cybersecurity**

December 2023

AGENDA

- About GAO
- GAO's Cybersecurity Related Work
- New Cybersecurity Program Audit Guide
- Feedback
- Q & A



Source: GAO

FISCAL YEAR 2023 ACCOMPLISHMENTS

By the Numbers: A look at our FY 2023 accomplishments



\$70.4 billion
in financial benefits



about \$84 return
for each \$1 of our budget



1,345
new recommendations



1,220
improvements in federal
government operations



671
total products



57
testimonies



about 2,000
bid protests
handled



over 700
legal decisions and
opinions issued

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.

ITC'S PORTFOLIO



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>

GAO MEDIA MENTIONS

- [Homeland Security Today: GAO Highly Critical of DHS's New Biometric Program](#) (September 26, 2023)
- [MeriTalk: GAO Flags IRS Cybersecurity Improvement for Fifth Straight Year](#) (August 8, 2023)
- [Politico: Government Watchdog Finds U.S. Embassies Running Software Vulnerable to Attacks](#) (August 4, 2023)
- [MeriTalk: GAO Chides NNSA for Pace in Addressing Cyber Threats](#) (June 13, 2023)
- [Federal News Network: Federal Prison System, Cybersecurity, Human Capital and More on GAO's High Risk List](#) (April 20, 2023)

GAO CYBERSECURITY BLOG POSTS



Improving Communication Could Strengthen Federal Efforts to Prevent the Next Major Cyberattack

SEPTEMBER 27, 2023

We've already seen what can happen when one of the nation's critical services is disrupted by a ...



The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be

AUGUST 29, 2023

Cybercrimes in the United States have resulted in hundreds of billions of dollars in losses, and ...



After a Recent Hacking —What are the Risks and Rewards of Cloud Computing Use by the Federal Government?

AUGUST 10, 2023

Cloud computing offers significant opportunities to increase government efficiency, as well as ...

Source: <https://www.gao.gov/blog>

GAO CYBERSECURITY WORK



Cybersecurity:
State Needs to Expediently
Implement Risk Management
and Other Key Practices.

[GAO-23-107012](#)

Published: Sept. 28, 2023

Personnel Vetting:
DOD Needs a Reliable Schedule
and Cost Estimate for the National
Background Investigation Services
Program.

[GAO-23-105670](#)

Published: Aug. 17, 2023

Cybersecurity Workforce:
National Initiative Needs to
Better Assess Its Performance.

[GAO-23-105945](#)

Published: July 27, 2023

POLL QUESTION

How much experience do you have in conducting cybersecurity audits?

- a) none
- b) 1-5 years
- c) 5-10 years
- d) 10+ years



U.S. GOVERNMENT
ACCOUNTABILITY
OFFICE

CYBERSECURITY PROGRAM AUDIT GUIDE

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

(GAO-23-104705)

**Asset and risk
management**



**Identity
and access
management**



**Incident
response**



**Configuration
management**



**Continuous
monitoring
and logging**



**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.



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

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)

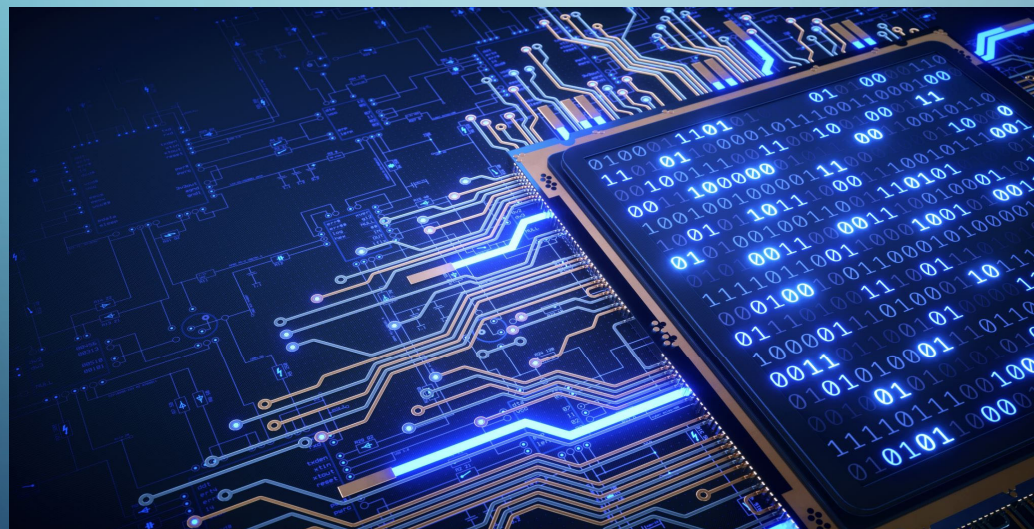
- FISCAM provides a methodology for assessing information system controls related to financial audits or attestation engagements.
- FISCAM was issued in 1999 and updated in 2009. Recently, an exposure draft of FISCAM was issued in June 2023 (GAO-23-104975).
- This revision reorders FISCAM to follow GAO's 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 Office of Inspectors General, independent public accounting firms, and state auditors.
- Held 10 focus groups with internal and external stakeholders. The focus groups included senior GAO executives, IT managers, and analysts across GAO; federal Office of Inspectors General; Independent Public Accounting representatives; and state auditors.
- Interviewed officials from NIST, the Center for Internet Security, and ISACA, among others for their input and comments.
- Performed content analysis on focus groups 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.



POLL QUESTION

Which high-risk area is most needed to be in a Cybersecurity Audit Guide, according to your own experience?

- a) Risk management
- b) Safeguarding of sensitive data
- c) Protection of critical infrastructure
- d) Incident response
- e) Something else

CPAG STRUCTURE

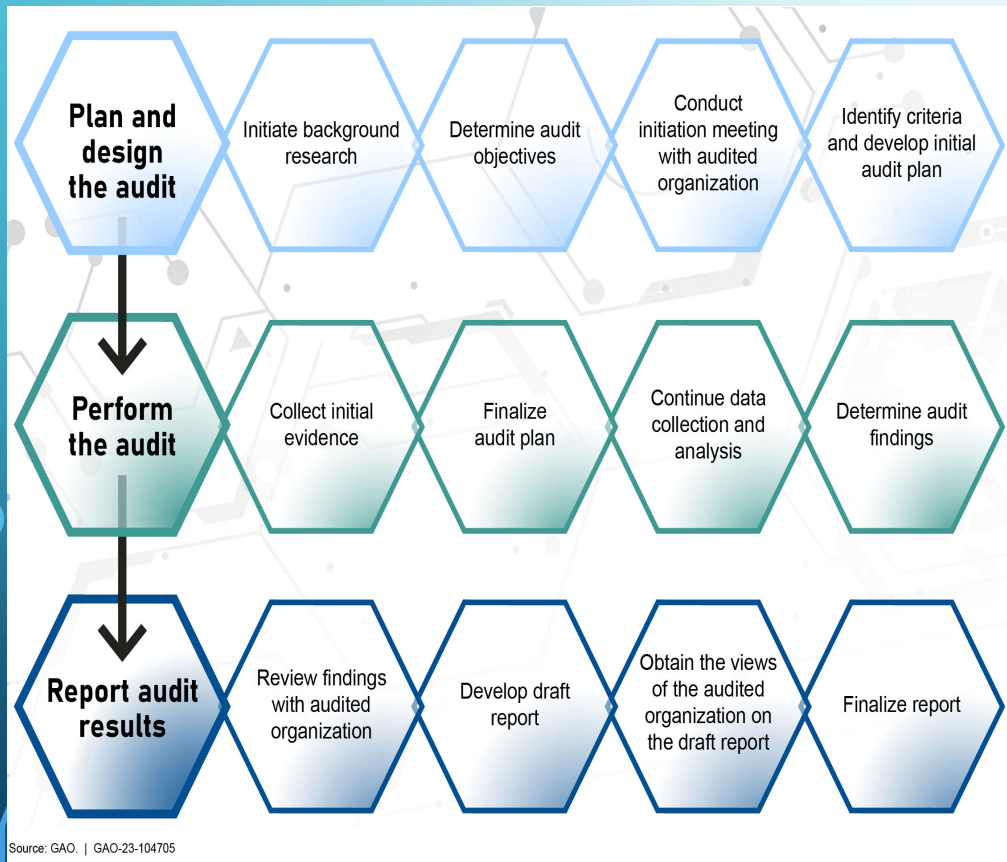
Chapter 1: general guide to the audit process

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



Source: GAO. | GAO-23-104705

- 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

CHAPTERS 2 TO 7: COMPONENTS

- Chapters 2 to 7 of CPAG



- 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.

Chapter 2. Asset and Risk Management Audit Steps



Source: GAO analysis of National Institute of Standards and Technology guidance; images: marinashvchenko/stock.adobe.com, pixtunz88/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 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 its network, including all authorized hardware and software, and data.

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

2.4 Review risk assessment: determine the extent to which the organization identifies the greatest risks, and manages which risks to accept and which to mitigate through security controls.

2.5 Review plans of actions and milestones: determine the extent to which the organization effectively documents planned remedial actions to correct deficiencies and vulnerabilities in the system.

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

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

Note: The use of "should" statements within key practices does not explicitly stated in criteria. Auditors using this guide should determine which key practices and audit steps to implement.

Example Controls and Audit Procedures for Asset and Risk Management

2.1 Assess IT Governance		
Control Objectives	Audit Procedures ^a	Examples of Control Criteria ^b
<p>2.1.1 Determine if the security control policies and procedures</p> <ul style="list-style-type: none"> are documented and appropriately consider risk; address purpose, scope, roles, responsibilities, and compliance; ensure that users can be held accountable for their actions; appropriately consider general and application controls; are approved by management; and are periodically reviewed and updated. 	<p>1. Review security policies and procedures and compare their content to NIST guidance and other applicable criteria. See if policies and procedures</p> <ul style="list-style-type: none"> consider risk; address purpose, scope, roles, responsibilities, and compliance; discuss that users are accountable for their actions; appropriately consider general and application controls; are approved by management; and are periodically reviewed and updated. <p>2. Review to see if security roles and responsibilities are defined. Roles and responsibilities may be defined in policies, job descriptions, agreements, hierarchy charts, and/or contracts.</p> <p>3. Analyze the contracts and service level agreements with critical vendors to determine if cybersecurity controls and incident notifications are addressed appropriately.</p>	<p>National Institute of Standards and Technology (NIST) SP 800-53 Revision 5: Risk Assessment (RA) RA-1 Policy and Procedures Assessment, Authorization and Monitoring (CA) CA-3 Information Exchange</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>
<p>2.1.2 Determine whether policies and procedures are implemented as intended.</p>	<p>1. Review security policies and procedures to ensure they include elements such as legal and regulatory requirements.</p> <p>2. Interview management personnel with information security and privacy responsibilities to determine whether policies and procedures are implemented as intended.</p> <p>3. For selected policies and procedures, determine the extent to which they are periodically tested for compliance and assess their enforcement.</p>	<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>

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 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



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

- **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



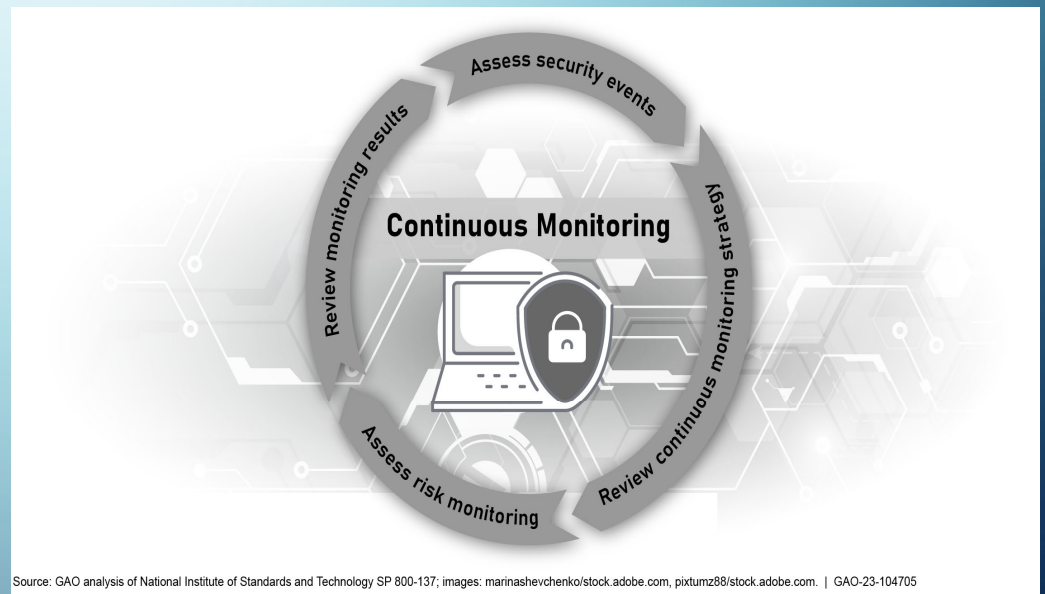
POLL QUESTION

Where have you seen the greatest vulnerabilities in physical security controls used to restrict access and protect resources from loss or impairment?

- a) Access control cards
- b) Fire warning & suppression
- c) Closed circuit cameras
- d) Security guards
- e) Something else

CHAPTER 5: CONTINUOUS MONITORING & LOGGING

- Involves maintaining ongoing awareness of cybersecurity, vulnerabilities, and threats occurring within an organization's systems and networks
- Discusses **5 key practices** for reviewing this component



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

CHAPTER 5: KEY PRACTICES

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

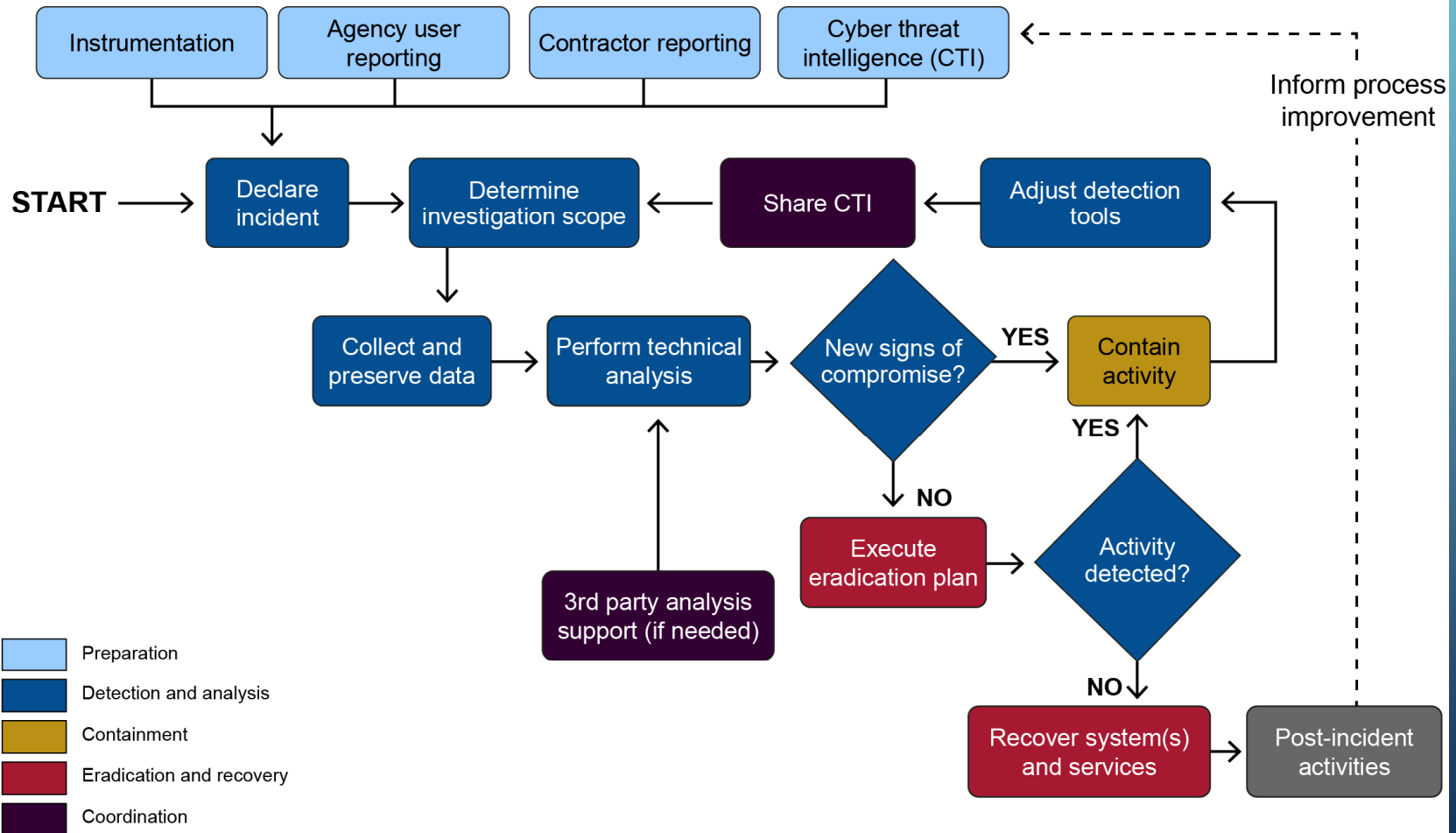
5.5 Assess Security Event Identification, Logging, and Retention



CHAPTER 6: INCIDENT RESPONSE

- Actions to take when actual or potential jeopardy to the confidentiality, integrity, or availability of systems or the information is identified.
- 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

CHAPTER 6: INCIDENT RESPONSE PROCESS



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

POLL QUESTION

A file that contains critical password information has been leaked at an information security organization. What is the best type of contingency plan for this situation, based on your past experience?

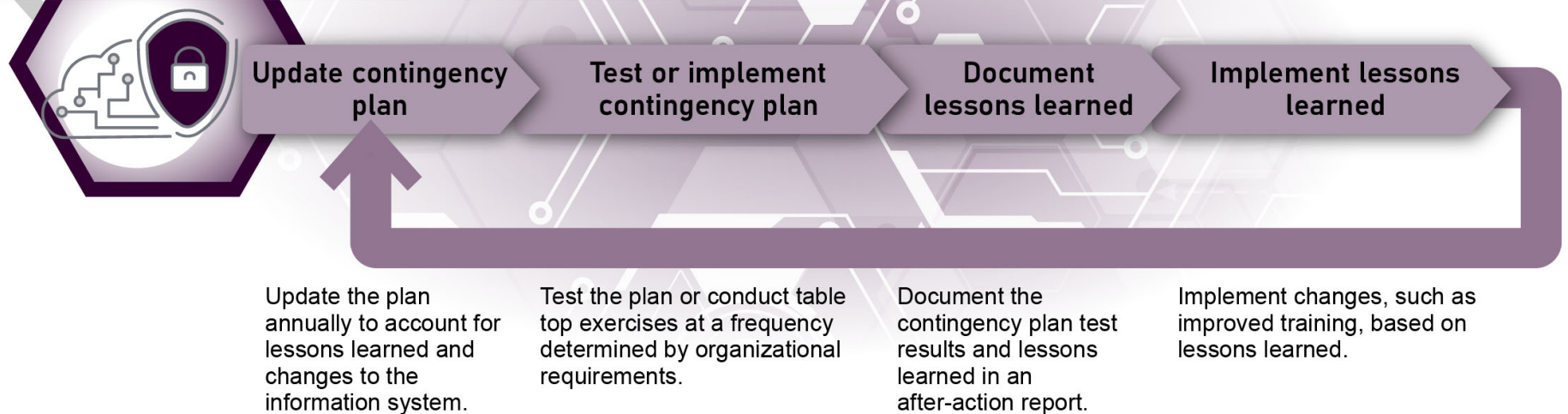
- a) Incident response plan
- b) Disaster recovery plan
- c) Continuity of operations plan
- d) Business continuity plan

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

CHAPTER 7: CONTINGENCY PLANNING AND RECOVERY PROCESS

Contingency planning and recovery



Source: GAO analysis of National Institute of Standards and Technology contingency planning guidance; images: marinashevchenko/stock.adobe.com, piktumz88/stock.adobe.com. | GAO-23-104705

POLL QUESTION

What kind of additional training regarding CPAG would you prefer?

- a) Live training
- b) Self-paced individual classes
- c) Real-world case studies that show implementation
- d) A mixture of all of the above

HAVE FEEDBACK?

- We plan to have revisions and updates for CPAG when the new NIST Cybersecurity Framework version 2.0 is published.
- Do you have any ideas on what else we should include?

Team's mailbox:

CPAG@gao.gov

- **Vijay 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

Chuck Young, Managing Director, YoungC1@gao.gov
(202) 512-3823, 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.