GAO's High-Risk Area: Ensuring the Cybersecurity of the Nation

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

May 2023

GAO High-Risk List

- In 1990, GAO began a program to report on government operations that we identified as “high risk.” Since then, generally coinciding with the start of each new Congress, we have reported on the status of progress to address high risk areas and update the High Risk List.

GAO’s Early Cybersecurity Days

- Between 1993 and 1997, we issued over 30 reports describing serious information security weaknesses at major federal agencies. For example:
  - In May 1996, we reported that tests at the Department of Defense showed that its systems may have experienced as many as 250,000 attacks during 1995, that about 64 percent of attacks were successful at gaining access, and that only a small percentage of these attacks were detected.
  - Many of the federal information security weaknesses and causal factors reported over those years were identified as a direct result of the annual financial statement audits initiated under the Chief Financial Officers Act of 1990.

GAO

1997: Cybersecurity Added to High Risk List

- When introducing information security to the High Risk list in 1997, we pointed out several related problems that needed to be addressed to help ensure that federal agencies adequately protected their systems and data:
  - Insufficient awareness and understanding of information security risks among senior agency officials
  - Poorly designed and implemented security programs that do not adequately monitor controls or proactively address risk
  - A shortage of personnel with the training and technical expertise needed to manage security controls in today’s sophisticated information technology environment

2003: High Risk Area Expands to Include Critical Infrastructure Cybersecurity

- In our 2003 high-risk update report, we broadened the high-risk area to include critical infrastructure cybersecurity because
  - failure to adequately protect these infrastructures could have consequences for national security, national economic security, and/or national public health and safety;
  - terrorist groups and others have stated their intentions of attacking our critical infrastructures;
  - federal influence over the private sector’s management of our nation’s critical infrastructures poses unique challenges; and
  - further actions on GAO’s related recommendations were needed, including (1) developing a national CIP strategy, (2) improving analysis and warning capabilities, and (3) improving information sharing on threats and vulnerabilities.

2015: High Risk Area Expands to Include Protecting Personally Identifiable Information

- In our 2015 high-risk update report, we noted that advancements in technology had made it easier for individuals and organizations to correlate data and track it across large and numerous databases.
- Furthermore, the number of reported security incidents involving personally identifiable information (PII) at federal agencies had increased significantly in recent years and a number of high-profile breaches of PII had occurred at commercial entities.
- We previously noted that no overarching federal privacy law governed the collection and sale of personal information among private sector companies, including information resellers.

2018: High Risk Area Emphasizes the Urgency of Ensuring the Cybersecurity of the Nation

- In September 2018, we updated the cybersecurity high-risk area by identifying four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them.
- A key emphasis of the update on the need for the federal government to develop and executive a comprehensive national strategy and to perform effective oversight.

Cybersecurity High Risk Area

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.

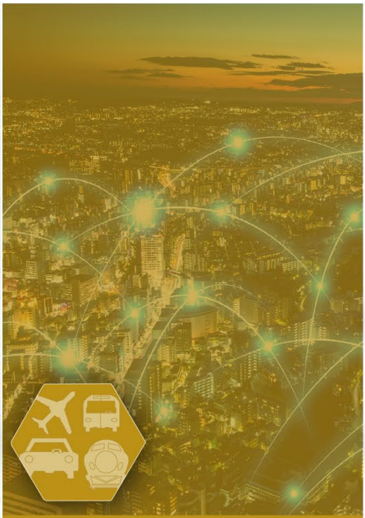
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5 Improve implementation of government-wide cybersecurity initiatives.

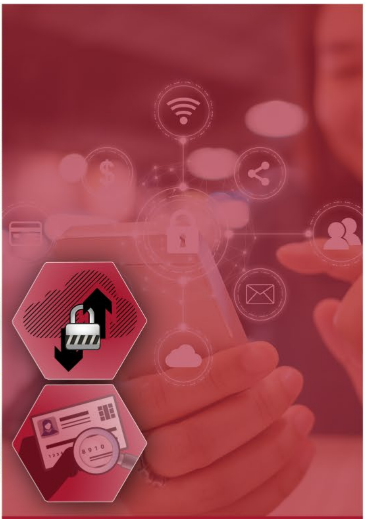
6 Address weaknesses in federal agency information security programs.

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.

Cybersecurity High Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight (GAO-23-106415)

The federal government should do the following:

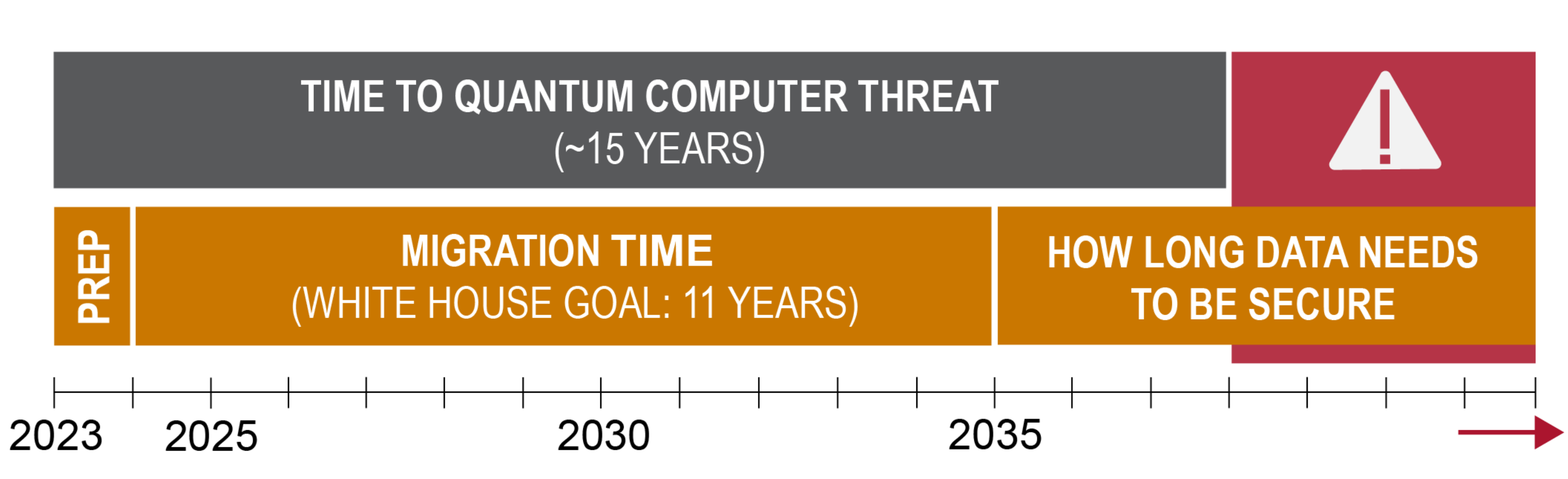
Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace

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

Address cybersecurity workforce management challenges

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

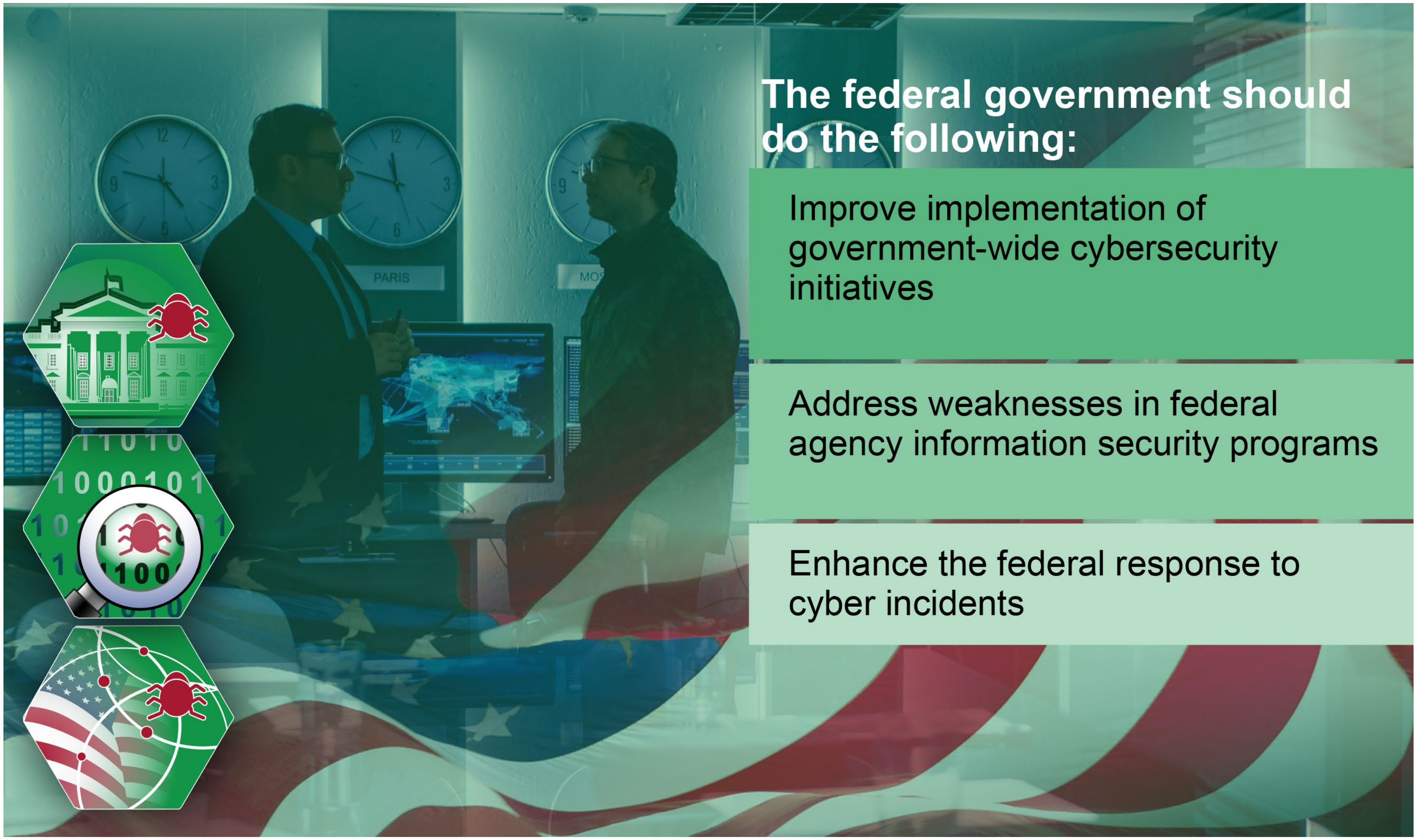
Cybersecurity High Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight (GAO-23-106415)


TIME TO QUANTUM COMPUTER THREAT
(~15 YEARS)
PREP
MIGRATION TIME
(WHITE HOUSE GOAL: 11 YEARS)
HOW LONG DATA NEEDS TO BE SECURE
2023
2025
2030
2035

🟥 Data unprotected

Source: GAO adaptation of Mosca’s theorem. | GAO-23-106559

Cybersecurity High Risk Series: Challenges in Securing Federal Systems and Information (GAO-23-106428)



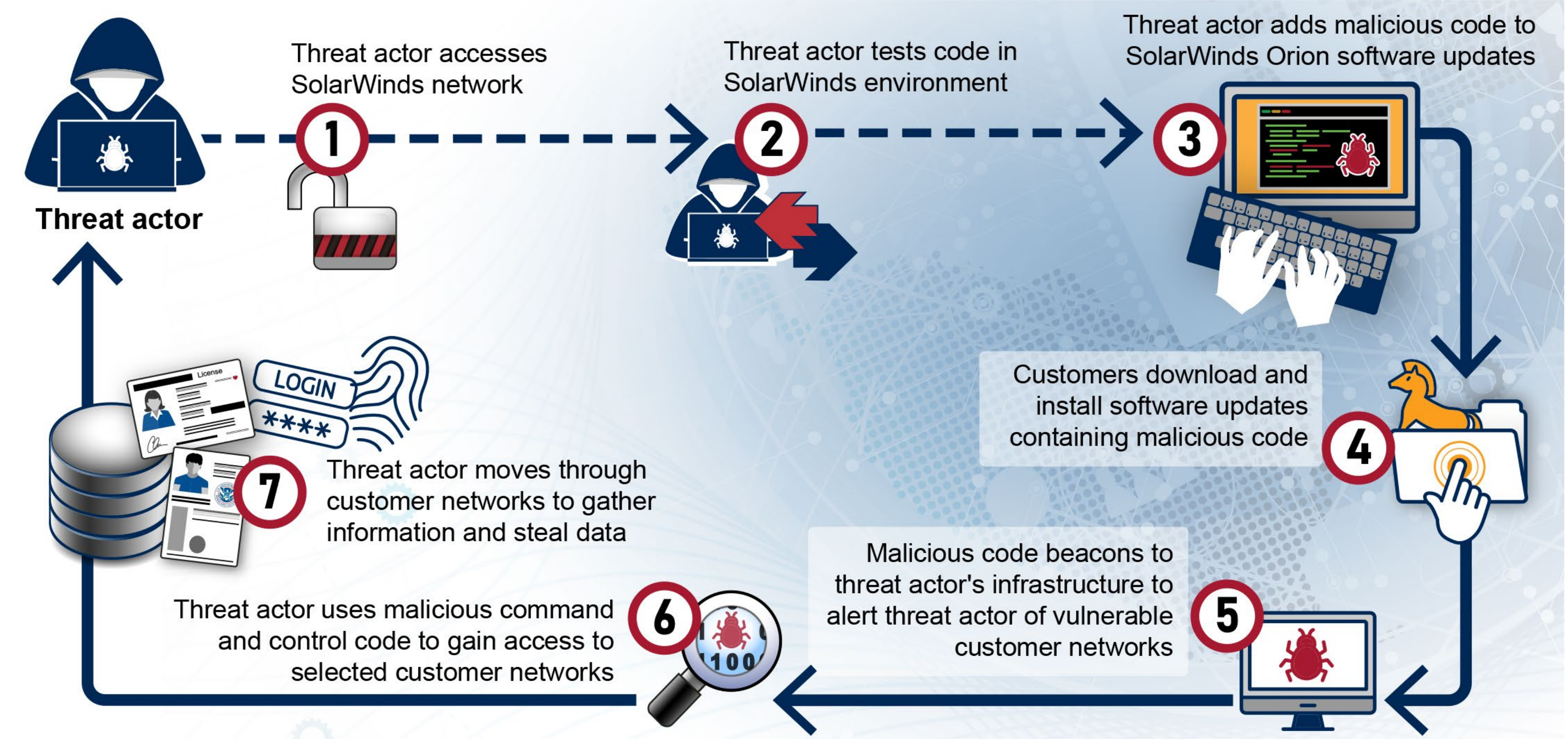
The federal government should do the following:

Improve implementation of government-wide cybersecurity initiatives

Address weaknesses in federal agency information security programs

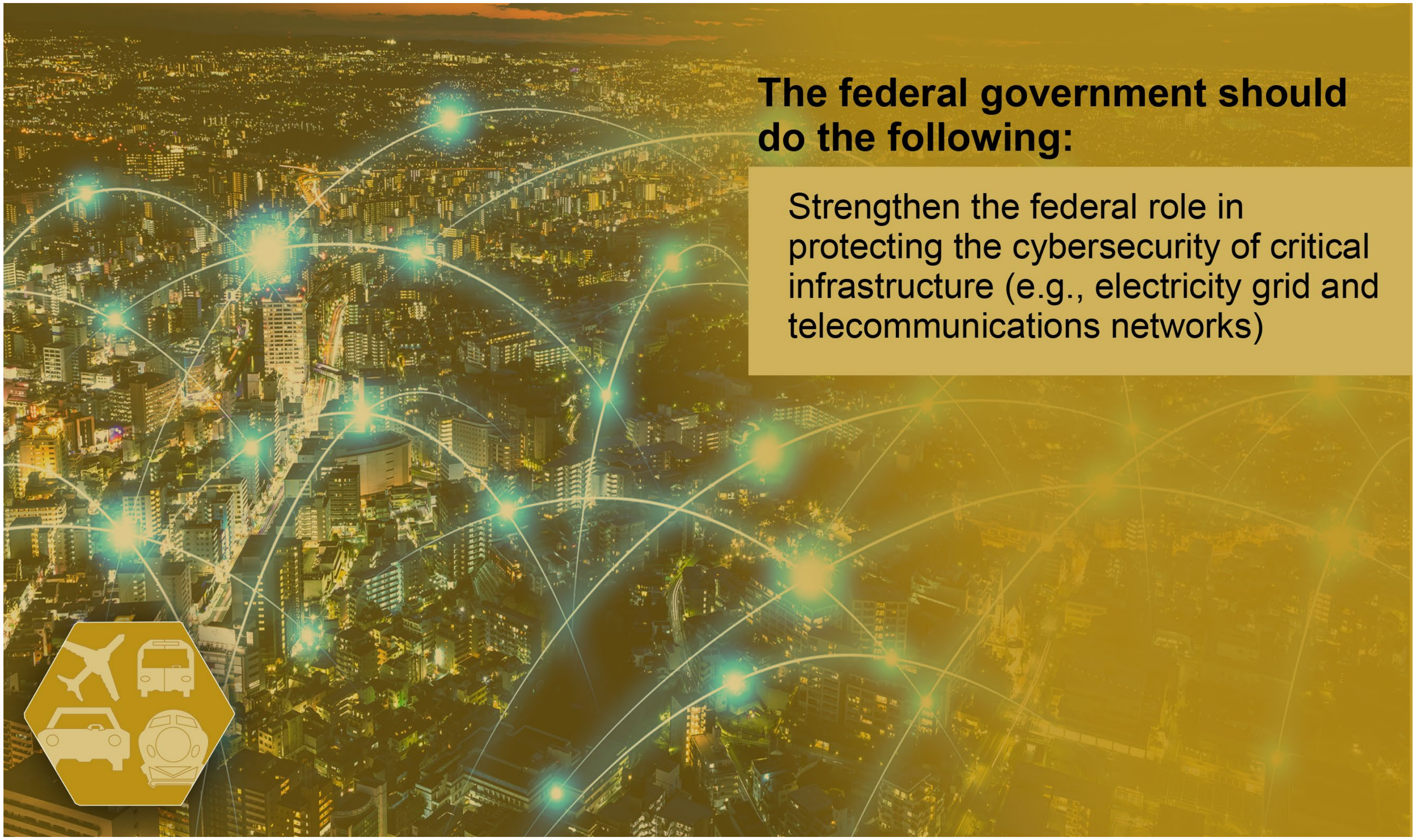
Enhance the federal response to cyber incidents

Cybersecurity High Risk Series: Challenges in Securing Federal Systems and Information (GAO-23-106428)


Threat actor
1 Threat actor accesses SolarWinds network
2 Threat actor tests code in SolarWinds environment
3 Threat actor adds malicious code to SolarWinds Orion software updates
4 Customers download and install software updates containing malicious code
5 Malicious code beacons to threat actor's infrastructure to alert threat actor of vulnerable customer networks
6 Threat actor uses malicious command and control code to gain access to selected customer networks
7 Threat actor moves through customer networks to gather information and steal data
LOGIN
****
License
100

Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-23-106428

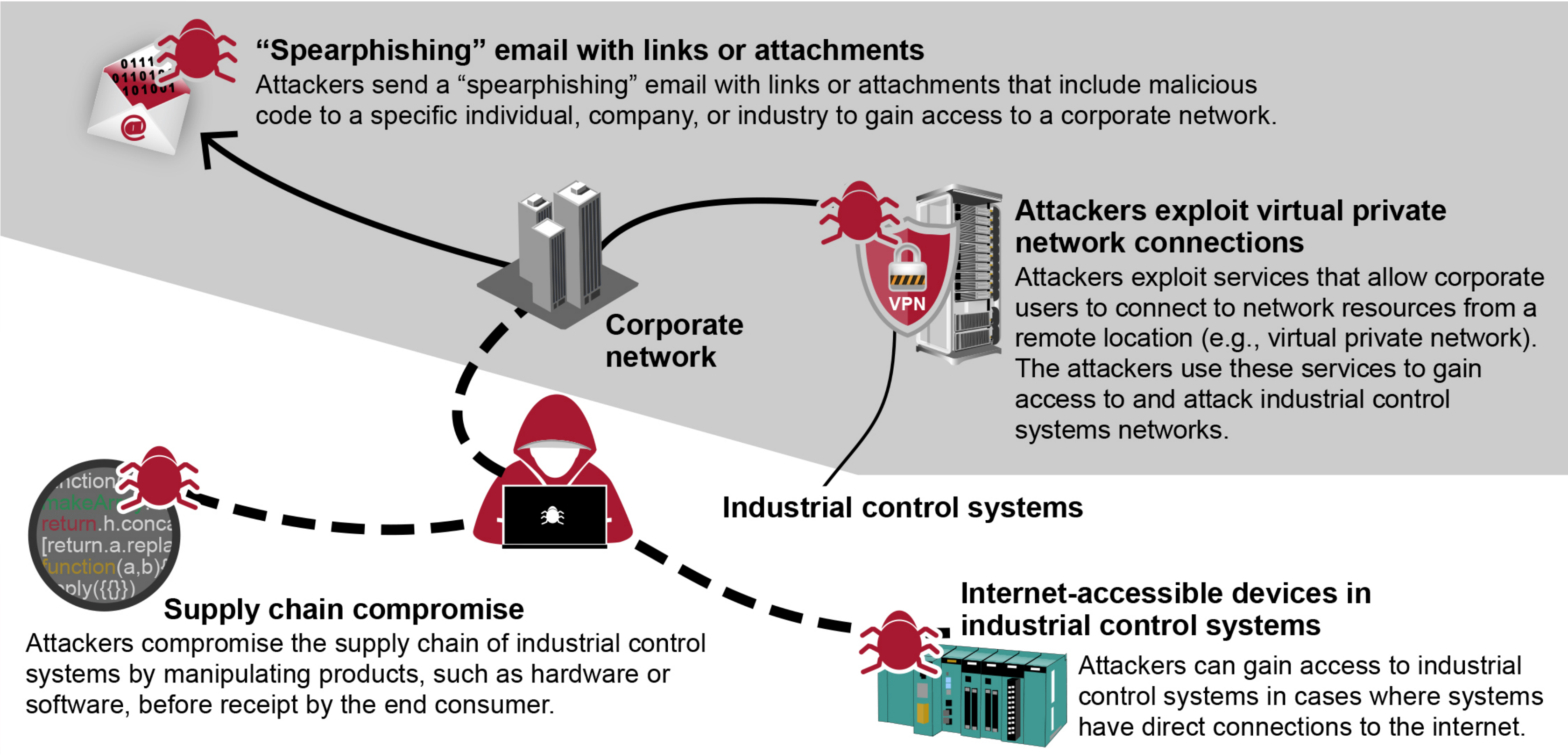
Cybersecurity High Risk Series: Challenges in Protecting Cyber Critical Infrastructure (GAO-23-106441)



The federal government should do the following:

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

Cybersecurity High Risk Series: Challenges in Protecting Cyber Critical Infrastructure (GAO-23-106441)



"Spearphishing" email with links or attachments
Attackers send a "spearphishing" email with links or attachments that include malicious code to a specific individual, company, or industry to gain access to a corporate network.

Corporate network

Attackers exploit virtual private network connections
Attackers exploit services that allow corporate users to connect to network resources from a remote location (e.g., virtual private network). The attackers use these services to gain access to and attack industrial control systems networks.

Industrial control systems

Supply chain compromise
Attackers compromise the supply chain of industrial control systems by manipulating products, such as hardware or software, before receipt by the end consumer.

Internet-accessible devices in industrial control systems
Attackers can gain access to industrial control systems in cases where systems have direct connections to the internet.

Source: GAO analysis of industry and federal documents. | GAO-23-106441

Cybersecurity High Risk Series: Challenges in Protecting Privacy and Sensitive Data (GAO-23-106443)

The federal government should do the following:

Improve federal efforts to protect privacy and sensitive data

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

Cybersecurity High Risk Series: Challenges in Protecting Privacy and Sensitive Data (GAO-23-106443)

Types of photos used by federal agencies that employ law enforcement officers

Federal agencies reported using a number of systems with facial recognition technology. The following list includes examples of the types of photos included in these systems, as reported by system owners and users:

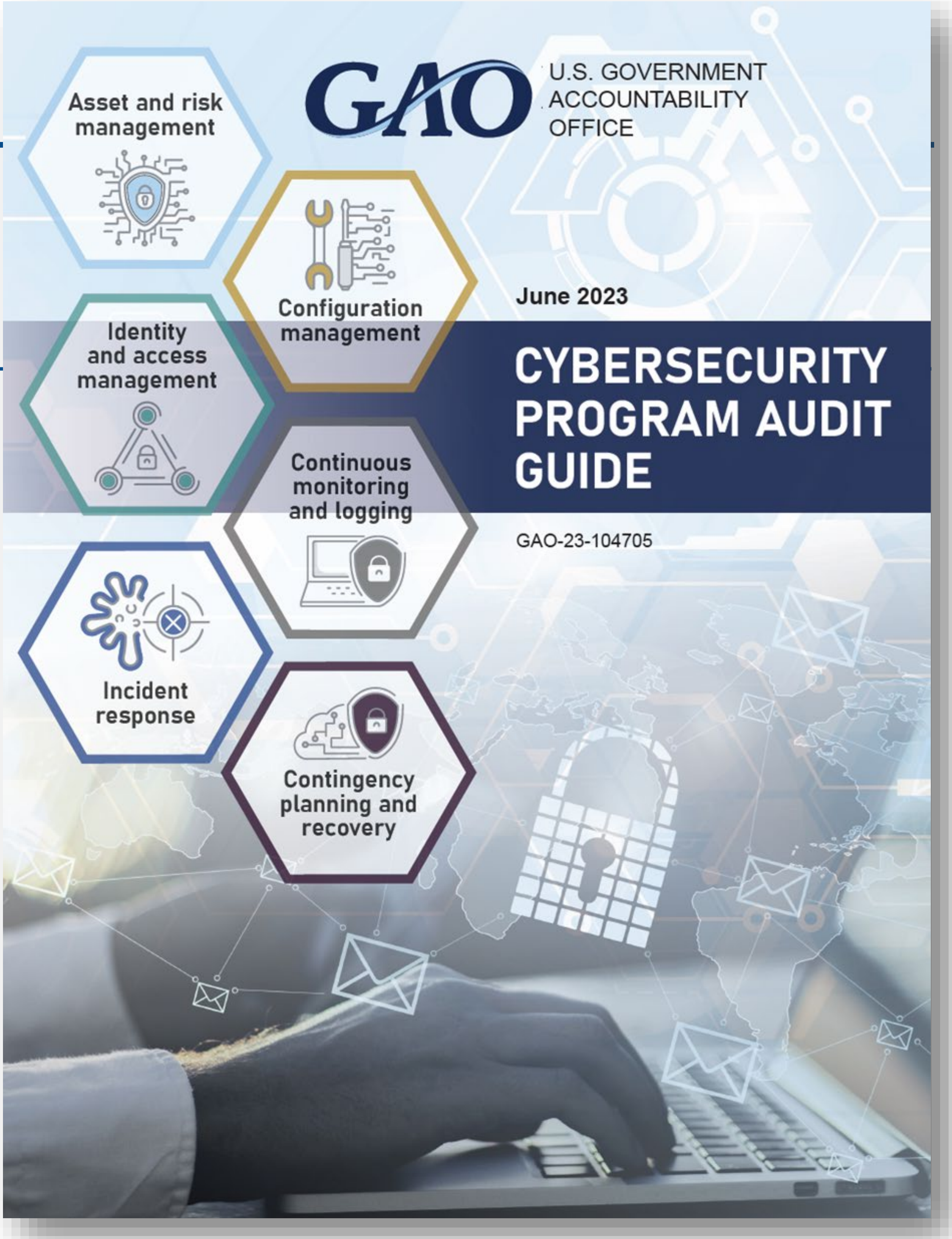
- Mug shot
- Publicly available on the internet
- Passport
- Visa application
- U.S. entry/exit
- Video/closed circuit television
- Terrorist screening database
- Foreign nationals and U.S. citizens who are known or suspected threats to the nation
- Employee
- State identification
- Driver's license
- Corrections identification
- Individuals under supervision

Source: GAO analysis of survey data; images: lidiia/stock.adobe.com. I GAO-23-106443

Coming soon!

Cybersecurity Program Audit Guide (CPAG)

Summer 2023



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

June 2023

CYBERSECURITY PROGRAM AUDIT GUIDE

GAO-23-104705

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

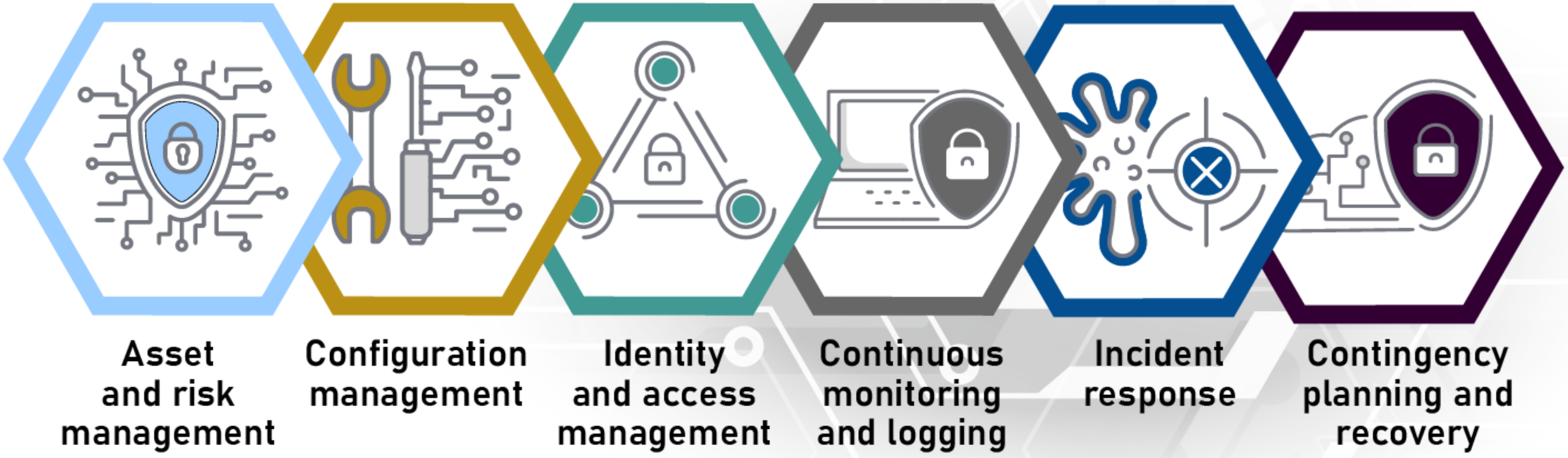
Coming soon!
Cybersecurity Program Audit Guide (CPAG)

- Intended to provide cyber analysts and auditors with a set of methodologies, techniques, and audit procedures to evaluate components of agency cybersecurity programs and systems.
- Relies on many 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.
- Will include an e-supplement containing examples of audit procedures for six primary components to include risk management, access management, incident handling, etc.

GAO

Draft Outline Structure

- **Chapter 1.** General guide to the audit process and the main phases of a performance audit focused on cybersecurity.
- **Chapter 2 to 7.** CPAG has 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

Draft Outline

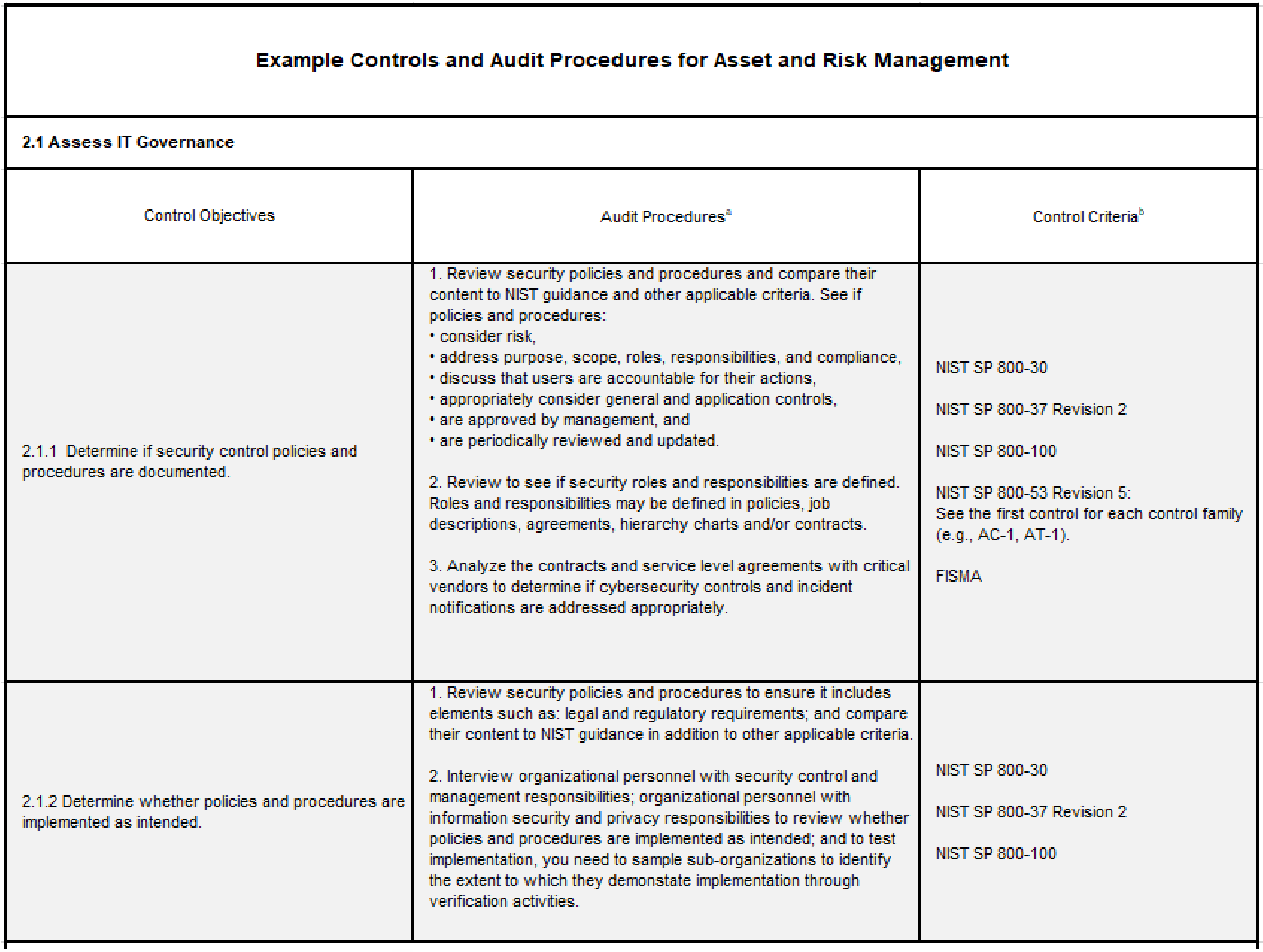
- **Chapter 2.** Asset and risk management—developing an organizational understanding of the cyber risks to assets, systems, information, and operational capabilities.
- **Chapter 3.** Configuration management—identifying and managing security features for system hardware, software, and firmware; and controlling changes to the configuration.
- **Chapter 4.** Identity and access management—protecting computer resources from modification, loss, and disclosure by limiting authorized access and detecting unauthorized access.
- **Chapter 5.** Continuous monitoring and logging—maintaining ongoing awareness of cybersecurity vulnerabilities and threats to an organization's systems and networks.

Draft Outline… *Continued*

- **Chapter 6.** Incident response—taking action when actual or potential security incidents occur.
- **Chapter 7.** Contingency planning and recovery—developing contingency plans and executing successful restoration of capabilities.
- **Appendix I.** A list of the criteria and additional resources used in the guide and e-supplement.
- **E-supplement.** Illustrative examples of controls and procedures are included for chapters 2-7.

CPAG E-Supplement Sample

Chapter 2: Asset and Risk Management



Example Controls and Audit Procedures for Asset and Risk Management		
2.1 Assess IT Governance		
Control Objectives	Audit Procedures[a]	Control Criteria[b]
2.1.1 Determine if security control policies and procedures are documented.	1. Review security policies and procedures and compare their content to NIST guidance and other applicable criteria. See if policies and procedures: • 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. 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. 3. Analyze the contracts and service level agreements with critical vendors to determine if cybersecurity controls and incident notifications are addressed appropriately.	NIST SP 800-30 NIST SP 800-37 Revision 2 NIST SP 800-100 NIST SP 800-53 Revision 5: See the first control for each control family (e.g., AC-1, AT-1). FISMA
2.1.2 Determine whether policies and procedures are implemented as intended.	1. Review security policies and procedures to ensure it includes elements such as: legal and regulatory requirements; and compare their content to NIST guidance in addition to other applicable criteria. 2. Interview organizational personnel with security control and management responsibilities; organizational personnel with information security and privacy responsibilities to review whether policies and procedures are implemented as intended; and to test implementation, you need to sample sub-organizations to identify the extent to which they demonstate implementation through verification activities.	NIST SP 800-30 NIST SP 800-37 Revision 2 NIST SP 800-100

WGITA - IDI Handbook on IT Audit

- Originally developed in 2014, the handbook is intended to provide guidance on the different domains of IT auditing, including information security.
- Between 2020 and 2022, GAO, in coordination with the INTOSAI Working Group on IT Audit (WGITA), the INTOSAI Development Initiative (IDI), and SAI India, worked on updates and enhancements to the handbook.
- The updated handbook was issued in March 2023.

INTOSAI IDI DEVELOPMENT INITIATIVE

INTOSAI Working Group on IT Audit

WGITA – IDI HANDBOOK ON IT AUDIT FOR SUPREME AUDIT INSTITUTIONS

Version 2022

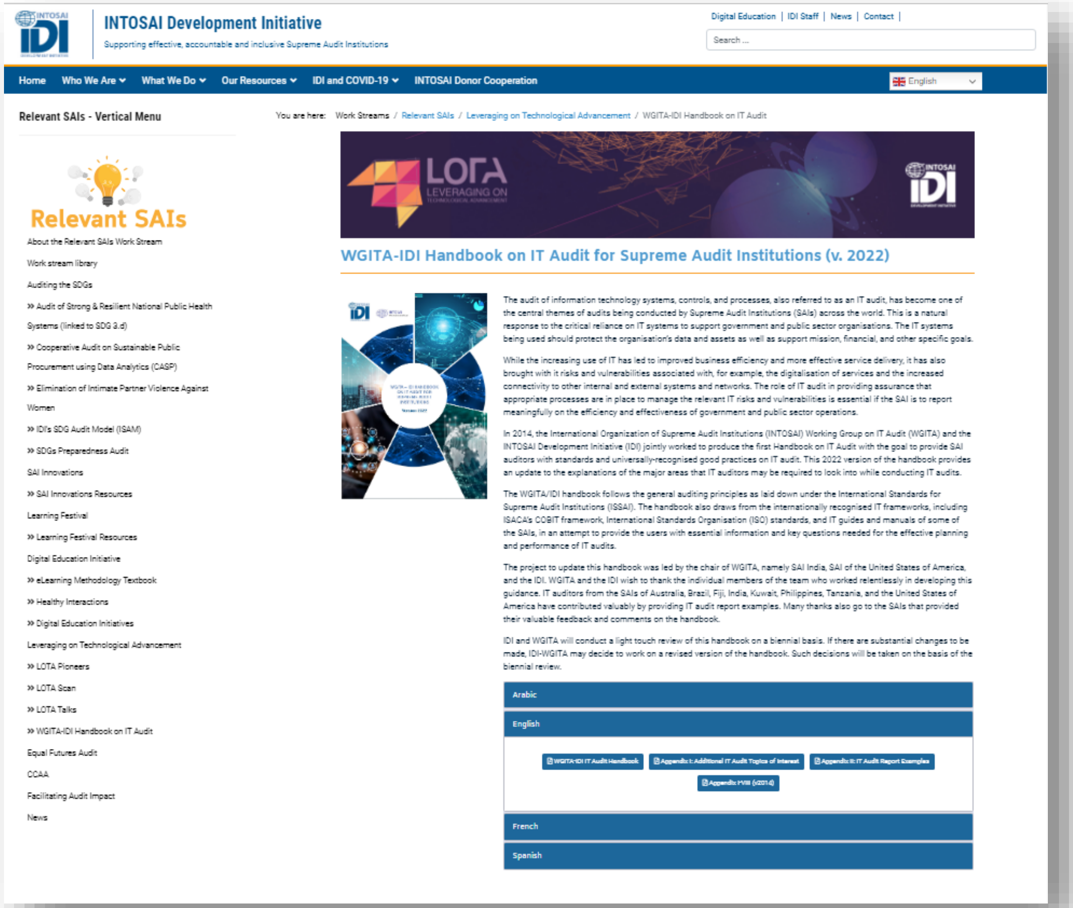
WGITA - IDI Handbook on IT Audit

- The eight primary handbook chapters cover different IT domain areas, such as:
  - IT governance and management,
  - outsourcing,
  - business continuity management, and
  - information security.
- For each IT domain area, the handbook provides an overview, key elements of the area, audit risk considerations, and additional information resources for further reading.
- Because of its significance to all areas of auditing, each of the IT domain areas touch on key IT security aspects and/or potential IT security risks to an organization for auditors to consider.

WGITA - IDI Handbook on IT Audit

- The updated handbook is available via IDI's website (www.idi.no) by searching for "Handbook on IT Audit", or by following the link below:

  https://www.idi.no/work-streams/relevant-sais/lota/wgita-idi-handbook-on-it-audit


INTOSAI
IDI
INTOSAI Development Initiative
Supporting effective, accountable and inclusive Supreme Audit Institutions
Digital Education | IDI Staff | News | Contact |
Search ...
Home
Who We Are
What We Do
Our Resources
IDI and COVID-19
INTOSAI Donor Cooperation
English
Relevant SAIs - Vertical Menu
You are here: Work Streams / Relevant SAIs / Leveraging on Technological Advancement / WGITA-IDI Handbook on IT Audit
Relevant SAIs
About the Relevant SAIs Work Stream
Work stream library
Auditing the SDGs
» Audit of Strong & Resilient National Public Health Systems (linked to SDG 3.d)
» Cooperative Audit on Sustainable Public Procurement using Data Analytics (CASP)
» Elimination of Intimate Partner Violence Against Women
» IDI's SDG Audit Model (ISAM)
» SDGs Preparedness Audit
SAI Innovations
» SAI Innovations Resources
Learning Festival
» Learning Festival Resources
Digital Education Initiative
» eLearning Methodology Textbook
» Healthy Interactions
» Digital Education Initiatives
Leveraging on Technological Advancement
» LOTA Pioneers
» LOTA Scan
» LOTA Talks
» WGITA-IDI Handbook on IT Audit
Equal Futures Audit
CCAA
Facilitating Audit Impact
News
LOTA
LEVERAGING ON
INTOSAI
IDI

WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions (v. 2022)

The audit of information technology systems, controls, and processes, also referred to as an IT audit, has become one of the central themes of audits being conducted by Supreme Audit Institutions (SAIs) across the world. This is a natural response to the critical reliance on IT systems to support government and public sector organisations. The IT systems being used should protect the organisation's data and assets as well as support mission, financial, and other specific goals.

While the increasing use of IT has led to improved business efficiency and more effective service delivery, it has also brought with it risks and vulnerabilities associated with, for example, the digitalisation of services and the increased connectivity to other internal and external systems and networks. The role of IT audit in providing assurance that appropriate processes are in place to manage the relevant IT risks and vulnerabilities is essential if the SAI is to report meaningfully on the efficiency and effectiveness of government and public sector operations.

In 2014, the International Organization of Supreme Audit Institutions (INTOSAI) Working Group on IT Audit (WGITA) and the INTOSAI Development Initiative (IDI) jointly worked to produce the first Handbook on IT Audit with the goal to provide SAI auditors with standards and universally-recognised good practices on IT audit. This 2022 version of the handbook provides an update to the explanations of the major areas that IT auditors may be required to look into while conducting IT audits.

The WGITA/IDI handbook follows the general auditing principles as laid down under the International Standards for Supreme Audit Institutions (ISSAI). The handbook also draws from the internationally recognised IT frameworks, including ISACA's COBIT framework, International Standards Organisation (ISO) standards, and IT guides and manuals of some of the SAIs, in an attempt to provide the users with essential information and key questions needed for the effective planning and performance of IT audits.

The project to update this handbook was led by the chair of WGITA, namely SAI India, SAI of the United States of America, and the IDI. WGITA and the IDI wish to thank the individual members of the team who worked relentlessly in developing this guidance. IT auditors from the SAIs of Australia, Brazil, Fiji, India, Kuwait, Philippines, Tanzania, and the United States of America have contributed valuably by providing IT audit report examples. Many thanks also go to the SAIs that provided their valuable feedback and comments on the handbook.

IDI and WGITA will conduct a light touch review of this handbook on a biennial basis. If there are substantial changes to be made, IDI-WGITA may decide to work on a revised version of the handbook. Such decisions will be taken on the basis of the biennial review.

Arabic
English
WGITA-IDI IT Audit Handbook
Appendix I: Additional IT Audit Topics of Interest
Appendix II: IT Audit Report Examples
Appendix I-VIII (v2014)
French
Spanish

Thank you!