Agenda

- About GAO
- Discussion of Federal Information System Controls Audit Manual (FISCAM)
- New Cybersecurity Audit Methodology Manual
- Next steps
- Q & A
**GAO’s Core Values**

**MISSION VALUES:**

**Accountability**
Enhance the economy, efficiency, effectiveness, and credibility of the federal government

**Integrity**
Conduct professional, objective, fact-based, non-partisan, non-ideological, fair, and balanced work

**Reliability**
Produce timely, accurate, useful, clear, and candid products

**PEOPLE VALUES:**

**Valued**
Seek out and appreciate each person’s perspectives

**Respected**
Treat everyone with dignity

**Treated Fairly**
Foster a work environment that provides opportunities for all

Source: https://www.gao.gov
Diversity, Equity, and Inclusion

**Diversity**

is the representation of all our varied identities and differences, recognizing that each employee has layers of diversity, which together make each employee's perspective unique and essential to the success of GAO.

**Equity**

is the fair treatment, access, opportunity, and advancement for all GAO employees, while at the same time striving to identify and eliminate barriers that could prevent the full participation of any employee.

**Inclusion**

is the degree to which employees perceive that they are valued members of the GAO workforce through their need for belongingness.

Source: https://www.gao.gov
Fiscal Year 2021
Accomplishments

By the Numbers: A look at our FY 2021 accomplishments

- $66.2 billion in financial benefits
- $158 return for each $1 of our budget (5-year average)
- 1,602 new recommendations
- over 1,200 improvements in federal government operations
- 578 reports
- over 60 congressional testimonies
- about 2,000 bid protests handled
- over 500 legal decisions and opinions issued

Source: GAO-22-4SP
Recent GAO Blog Posts

Challenges in Mapping the Digital Divide
OCTOBER 19, 2021
The divide between those who had access to broadband and those who did not was highlighted during...

IRS’s Efforts to Modernize 60-year-old Tax Processing System Is Almost a Decade Away
NOVEMBER 04, 2021
IRS relies extensively on information technology (IT) to process tax returns, collect taxes...

Preventing Fraud in CARES Act Programs
NOVEMBER 16, 2021
Congress appropriated nearly $5 trillion through the Coronavirus Aid, Relief, and Economic Security...
Cybersecurity Work


Why is FISCAM being updated?
The 2009 FISCAM content has been reorganized to (1) follow the planning, testing, and reporting phases of an engagement and (2) move the tables containing the critical elements, control activities, control techniques, and audit procedures for each general and application control category to an appendix.

This appendix has tentatively been re-branded as the FISCAM objectives-based control framework or FISCAM framework.

- Section 100 – Introduction
- Section 200 – Planning
- Section 300 – Testing
- Section 400 – Reporting
- Section 500 – Appendices
FISCAM Time Frames

- Exposure Draft – anticipated release summer 2022
- Final Publication – TBD
Cybersecurity Audit Methodology Manual

Four major cybersecurity challenge areas

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

Source: GAO analysis
New and experienced auditors can use the new IT cybersecurity audit methodology manual for FISMA and cybersecurity related audits.

The control activities listed in this manual are consistent with: the NIST Cybersecurity Framework (CSF), NIST 800-53 Rev. 5, other NIST publications, and Office of Management and Budget cybersecurity control-related policies and guidance, among others.

The procedures listed in the Cybersecurity Audit Methodology Manual are intended to be flexible, provide a framework and starting point to assess the enhanced security requirements, and can be tailored to the needs of the auditor.
## Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crosswalks to the NIST Cybersecurity Framework and NIST 800-53 Rev. 5</td>
<td>Crosswalks to the NIST Cybersecurity Framework and NIST 800-53 Rev. 5 controls</td>
<td></td>
</tr>
<tr>
<td>Crosswalks to GAO’s Green Book and Yellow Book</td>
<td>Crosswalks to GAO’s Green Book and Yellow Book</td>
<td></td>
</tr>
<tr>
<td>NIST CSF-based suggested audit steps</td>
<td>NIST CSF-based suggested audit steps</td>
<td></td>
</tr>
</tbody>
</table>
Draft Outline

• **Chapter 1.** Use and Application. Who will use this manual and what is the purpose.

• **Chapter 2.** General Planning. How to plan for the audit.

• **Chapter 3.** Audit Steps. Suggested detail audits steps for areas such as: assets and risk management; protecting systems and information; logging and monitoring; incident response; and contingency planning.

• **Appendixes**
  • NIST CSF-based suggested audit steps (Excel spreadsheet)
  • Mapping NIST CSF to Green Book (Excel spreadsheet)
  • Mapping NIST CSF to other NIST publications
Challenges

Information Security vs. Cybersecurity

Criteria used (NIST 800-53 or NIST Cybersecurity Framework)

Detailed steps vs. high-level examples and concepts

Zero Trust Architecture

Cloud computing, FedRAMP, StateRAMP
Cybersecurity Audit Methodology Manual Time Frames

- Draft publication – beginning of 2022
- Final Publication – summer 2022
Differences between FISCAM and CAMM

- The *Federal Information System Controls Audit Manual (FISCAM)* revision will continue to support assessing information system controls related to financial audits, attestation engagements, and certain performance audits.

- The *Cybersecurity Audit Methodology Manual* will support both information security and cybersecurity performance audits.
Have Feedback?

Team’s mailbox:
CybersecurityAuditManualUpdate@gao.gov

• Jennifer R. Franks, FranksJ@gao.gov
• Tammi Kalugdan, KalugdanT@gao.gov
• Rosanna Guerrero, GuerreroR@gao.gov
Thank you!