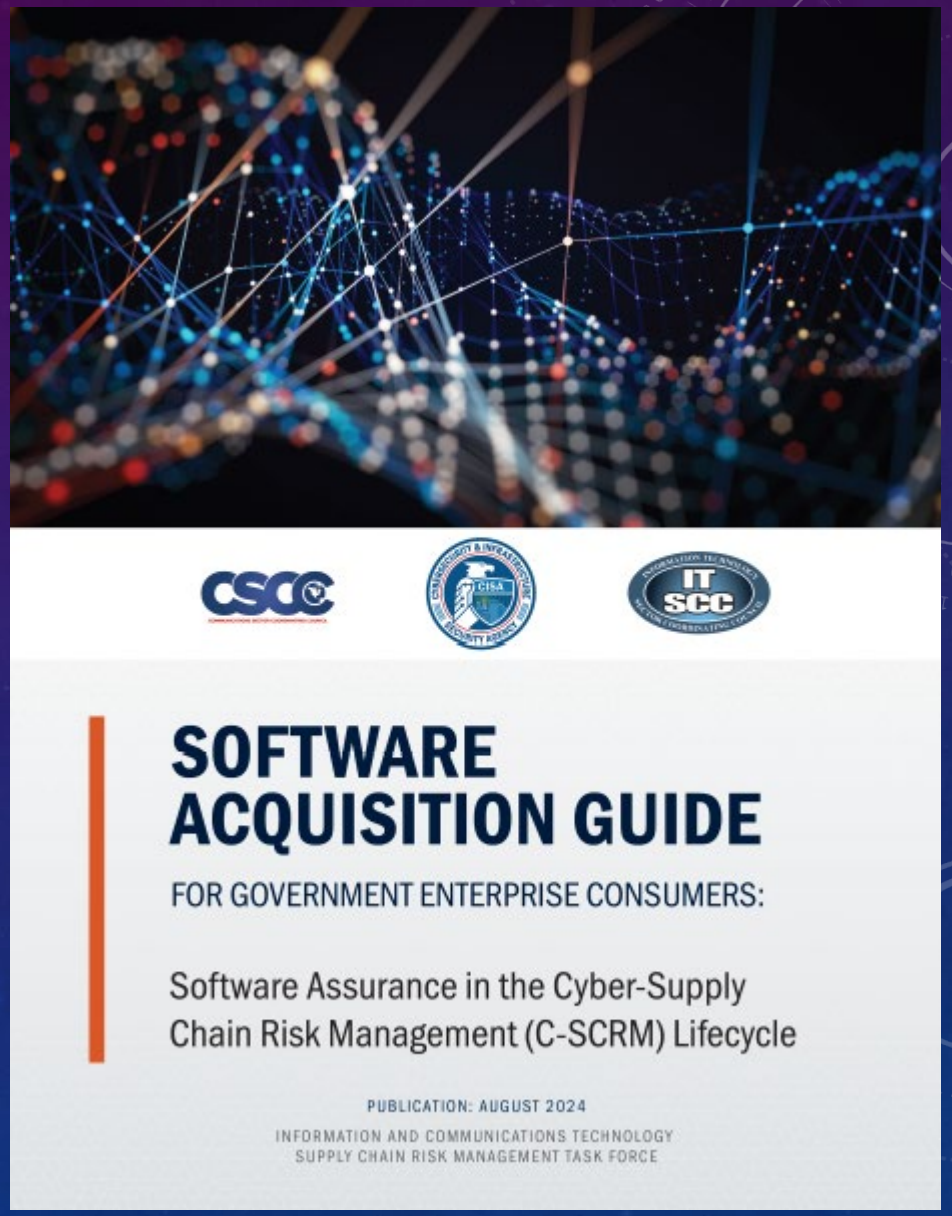
CISA SECURE BY DESIGN SOFTWARE ACQUISITION GUIDE (SAG)

BEST PRACTICES TO VERIFY PRODUCTS FOR SECURE BY DESIGN AND SECURE BY DEFAULT

TOPICS

- What is the CISA Software Acquisition Guide (SAG)
- Who created the SAG materials
- How do Product Manufacturers use the SAG
- How do Consumers use the SAG to assess a product for Secure by Design Best Practices
- Resources



WHAT IS THE CISA SOFTWARE ACQUISITION GUIDE

- Aligns with CISA Secure by Design principles but focuses on the “Secure by Demand” elements.
- Identifies Secure by Design best practices across the entire software life cycle
- Enables acquisition professionals to engage in more relevant discussions with their enterprise risk owners (such as Chief Information Officers and Chief Information Security Officers) and candidate suppliers
- A virtual “Secure by Design” checklist for consumers and producers

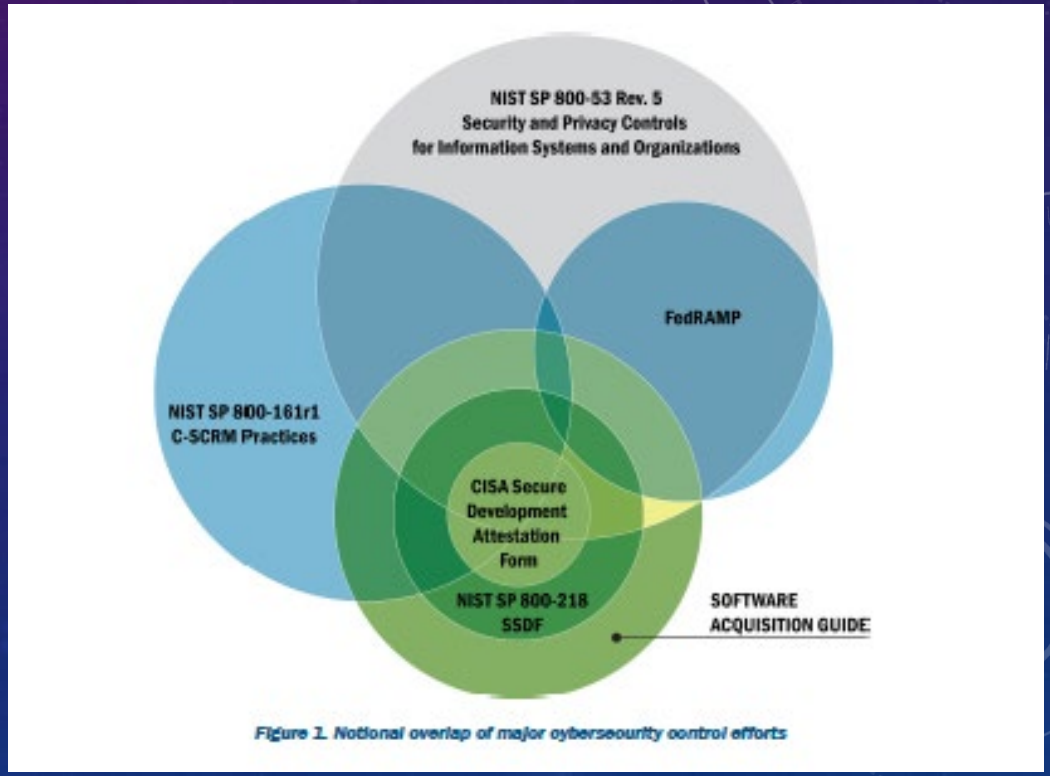


Figure 1. Notional overlap of major cybersecurity control efforts

View the CISA NASPO Webinar for a comprehensive overview

Software Acquisition Guide

This guide is organized into five primary sections with each section having its own set of controls and clarifying tasks, including:

- 19 CONTROL questions for Supplier Governance and Attestations
- 8 CONTROL questions for Software Supply Chain
- 30 CONTROL questions for Secure Software Development
- 12 CONTROL questions for Secure Software Deployment
- 8 CONTROL questions for Vulnerability Management

The questions are organized into a series of CONTROL questions with most CONTROL questions having a series of informative TASK questions. For each CONTROL question, it is expected that the software supplier will provide a simple response of “Yes,” “No,” “N/A,” or “Partial.”

WHO CREATED THE SAG MATERIALS

- CISA ICT_SCRM Task Force (CIPAC partnership)
- CISA National Risk Management Center
- Core group of ~30 people working on the SAG document
- Mostly from Government Agencies (NASA, GSA, CISA, NSA) and Private Sector https://www.cisa.gov/ict-scrm-task-force-members
- Led and facilitated by CISA personnel over two years
- Visionary leadership provided by an expert with decades of experience in software assurance, Joe Jarzombek, https://copilot.microsoft.com/shares/QLhY366t3XSbYmfegpXEa

ICT SCRM Task Force Members

The ICT SCRM Task Force is composed of a diverse range of representatives from large and small private sector organizations within the Information Technology (IT) and Communications sectors, ICT associations, and federal agencies. Members include subject matter experts, ICT sector owners and operators, and other key stakeholders who provide recommendations and guidance to help shape trusted supply chain practices.

Companies and organizations participating in the Task Force include:

SECURE BY DESIGN, DEFAULT, DEMAND

- *"'Secure by design' means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure."* (Source: Principles and Approaches, page 8) This sets an expectation for suppliers and includes how suppliers should take ownership of security outcomes for their customers, demonstrate radical transparency and accountability, and lead from the top by making secure by design a top business priority. This applies to the entire software development lifecycle (SDLC)/product lifecycle.

- *"'Secure by default' means products are resilient against prevalent exploitation techniques out of the box without added charge...without end-users having to take additional steps to secure them...make customers acutely aware when they deviate from safe defaults..."* (Source: Principles and Approaches, page 9) This means products come with a baseline level of security by default that do not need significant effort by customers to 'harden' the products and software against exploitation. The CISA guidance also states that, "The complexity of security configuration should not be a customer problem...," (Source: Principles and Approaches, page 9) and that customers are not charged extra for implementing added security configurations.

- *'Secure by demand' means customer expectations for secure software and products are articulated in acquisition and procurement activities and contracts.* Within government agencies, employees performing requirements and contracting functions have significant roles in communicating enterprise expectations for secure software. Agencies can provide more complete guidance to support their efforts to focus on obtaining secure software. Since it remains challenging for suppliers to make the required security investments and efforts without associated demand, the updated CISA guidance also emphasizes the need for consumer demand: *"...just as we seek to create a pervasive secure by design philosophy within software manufacturers, we need to create a 'secure by demand' culture with their customers."* (Source: Principles and Approaches, page 7) To focus on the need to correct market failures of cybersecurity, increased demand for secure products and software from enterprise customers and consumers is needed in acquisition and procurement because it is directly tied to customer demand and spending, which impacts supplier revenue and profits.

HOW DO PRODUCT MANUFACTURERS USE THE SAG

- Self Assessment of adherence to Secure by Design best practices in the SAG
- Perform self assessment before submitting a product to the US Government for procurement
- Answer the 19 Governance Questions, at a minimum
- Address any “red flags” where lack of adherence to Secure by Design could block a product from being purchased
- Create SAG Spreadsheet once and send to everyone that asks to show your Secure by Design practices
- Track Secure by Design practices per product

HOW DO CONSUMERS USE THE CISA SAG

- Assess a product and supplier for adherence to Secure by Design best practices
- Five step process
  1. Download the CISA SAG Spreadsheet
  2. Send the spreadsheet to your suppliers with a cover letter asking them to answer the 19 governance questions, at a minimum and return the completed spreadsheet
  3. Place the completed SAG Spreadsheets received in a permanent location for later review
  4. Evaluate each returned spreadsheet and decide if the provided responses are acceptable within your risk threshold and tolerance
  5. Keep a history of each analysis in a “log book” with PASS/FAIL results

POPULARITY

Reported metrics

From the CISA SSCA Forum slide deck:

Resource	Reported Clicks (as of Jan 23, year not specified)
Software Acquisition Guide (PDF)	**10,430**
Software Acquisition Guide Spreadsheet	~5,000

Sources: NIST Computer Security Resource Center

RESOURCES

- NASA SCRM Process Documentation
  - https://www.nasa.gov/secure-software-development-self-attestation-resources-and-knowledge/
- CISA SAG Videos
  - NASPO Webinar: https://www.youtube.com/watch?v=_RzQMXE4Df0
  - Tom Fanning Keynote: https://www.youtube.com/watch?v=0iYITlQfi3A
- CISA Free Services and Open Source Tools
  - https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools
  - https://github.com/rjb4standards/CISASAGReader/blob/main/README.md
- CISA SAG Website
  - https://cisa.gov/sag
  - SAG Document: https://www.cisa.gov/sites/default/files/2024-07/PDM24050%20Software%20Acquisition%20Guide%20for%20Government%20Enterprise%20ConsumersV2_508c.pdf
  - SAG Spreadsheet: https://www.cisa.gov/sites/default/files/2024-08/PDM24064%20Software%20Acquisition%20Guide%20for%20Government%20Enterprise%20Consumers%20Final-%2020240710_v19.xlsx
  - SAG FACT Sheet: https://www.cisa.gov/sites/default/files/2024-10/ICT%20SCRM%20Task%20Force%20Software%20Acquisition%20Guide%20Fact%20Sheet%20%28508%29.pdf
- LinkedIn SBOM SIG; Global Community of SBOM Implementers
  - https://www.linkedin.com/groups/13274064/

Thank you for your time

Dick Brooks
dick@businesscyberguardian.com
https://businesscyberguardian.com/