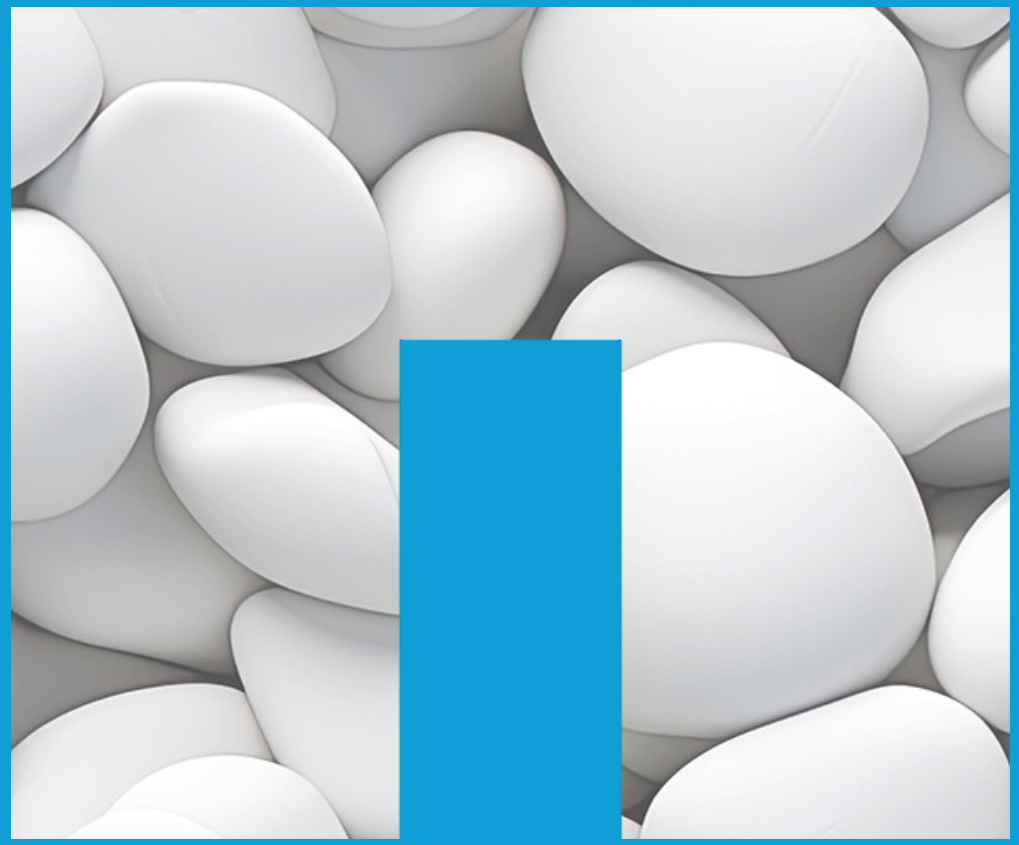
NetApp

SOFTWARE ACQUISITION GUIDE

SUPPLY CHAIN SECURITY ASSESSMENT



Sridhar Balasubramanian

Principal Security Architect, NetApp, Inc.,

October 2025

Agenda

- Motivation and Scope
- Notional overlap of major cybersecurity control efforts
- Use Cases
- Governance questions: Example
- Software Acquisition Guide Spreadsheet
- Demo: Software Acquisition Guide Online Survey Tool
- Secure by Design/Demand
- How NetApp uses this Guide?
- References

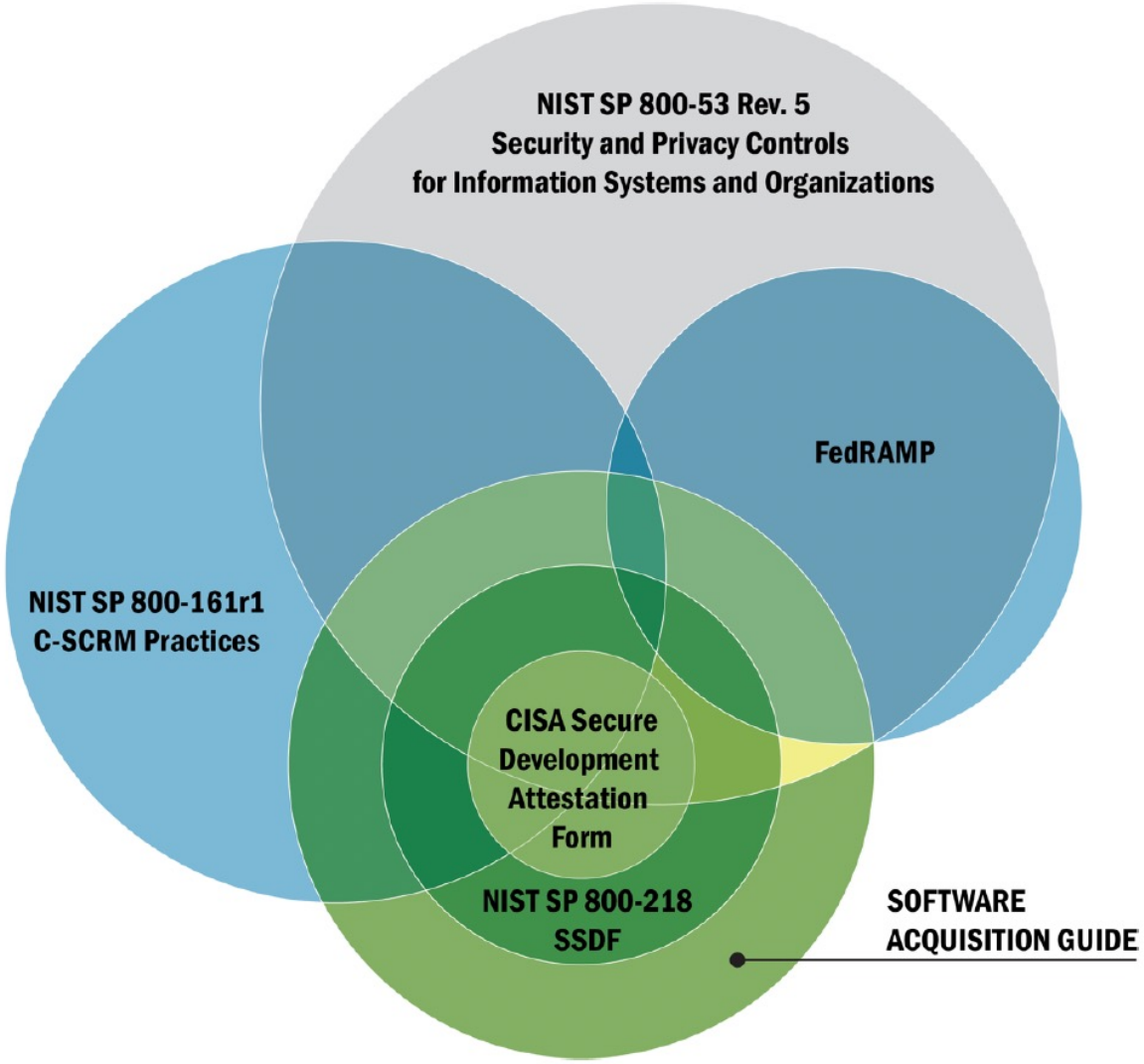
Motivation

- The level of transparency provided by suppliers of software and cyber-physical devices relative to their development and third-party management practices can make technology acquisitions challenging.
- The acquisition staff often lack the ability to assess whether a given supplier has practices and policies in place that better meet the ongoing expectations of enterprise users of the products.
- Intended audience for this guide include individuals in software acquisition roles supporting government agencies and suppliers of software.

Scope

- The Software Acquisition Guide aligns with the Cybersecurity and Infrastructure Security Agency's (CISA) Secure by Design principles but focuses on the "Secure by Demand" elements.
- By providing recommendations, this guide allows 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.

Notional Overlap of Major Cybersecurity Control Efforts



Organization of Software Acquisition Guide

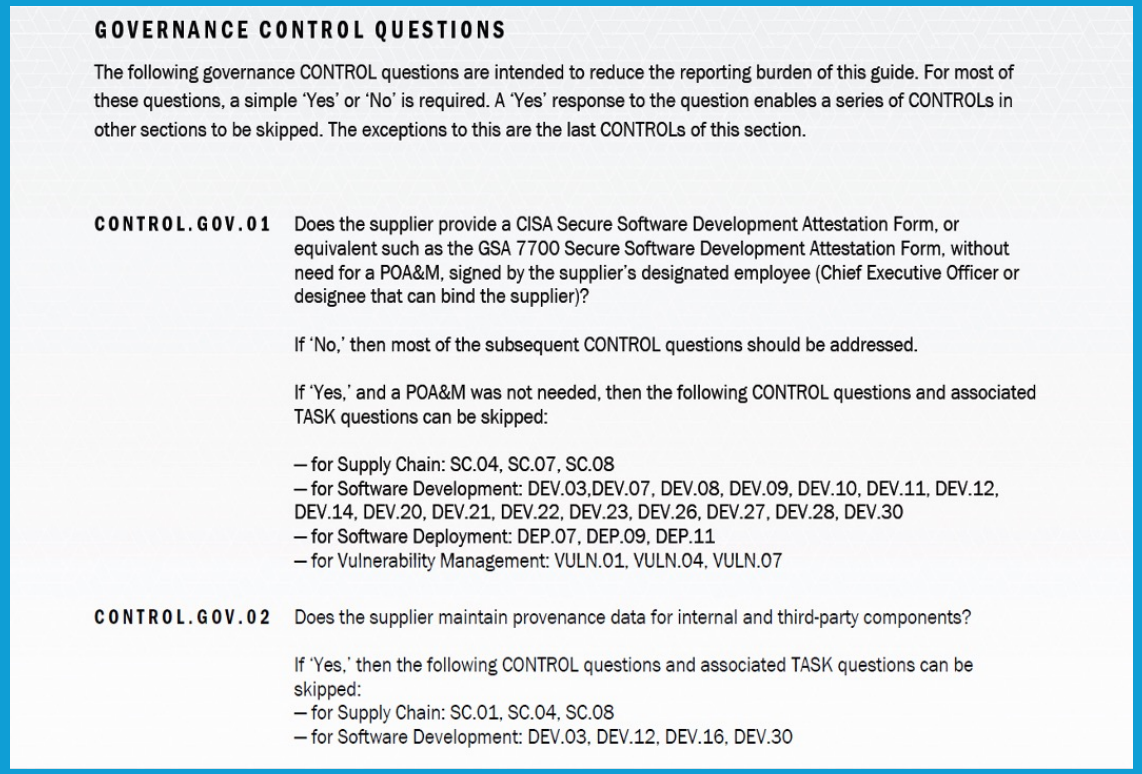
- This guide is organized into five primary sections with each section having its own set of controls and clarifying tasks, including:
  - 19 CONTROL questions for Supplier Governance and Attestations
  - 8 CONTROL questions for Software Supply Chain
  - 30 CONTROL questions for Secure Software Development
  - 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.”

Use Cases for Software Acquisition Guide

- Software Procurement Decisions
- Software Vendor Selection and Acceptance Criteria
- Software Vendor Onboarding Criteria
- Software Vendor Contract Negotiations and Renewals
- Software Supply Chain Risk Assessment
- Software Compliance and Certification

Governance questions - Example

- Total of 19 Governance questions
- Each Governance question shows what CONTROL questions can be skipped based on your response
- A “Yes” to all 19 Governance questions results in all CONTROL questions being skipped



GOVERNANCE CONTROL QUESTIONS

The following governance CONTROL questions are intended to reduce the reporting burden of this guide. For most of these questions, a simple ‘Yes’ or ‘No’ is required. A ‘Yes’ response to the question enables a series of CONTROLs in other sections to be skipped. The exceptions to this are the last CONTROLs of this section.

CONTROL.GOV.01 Does the supplier provide a CISA Secure Software Development Attestation Form, or equivalent such as the GSA 7700 Secure Software Development Attestation Form, without need for a POA&M, signed by the supplier’s designated employee (Chief Executive Officer or designee that can bind the supplier)?

If ‘No,’ then most of the subsequent CONTROL questions should be addressed.

If ‘Yes,’ and a POA&M was not needed, then the following CONTROL questions and associated TASK questions can be skipped:

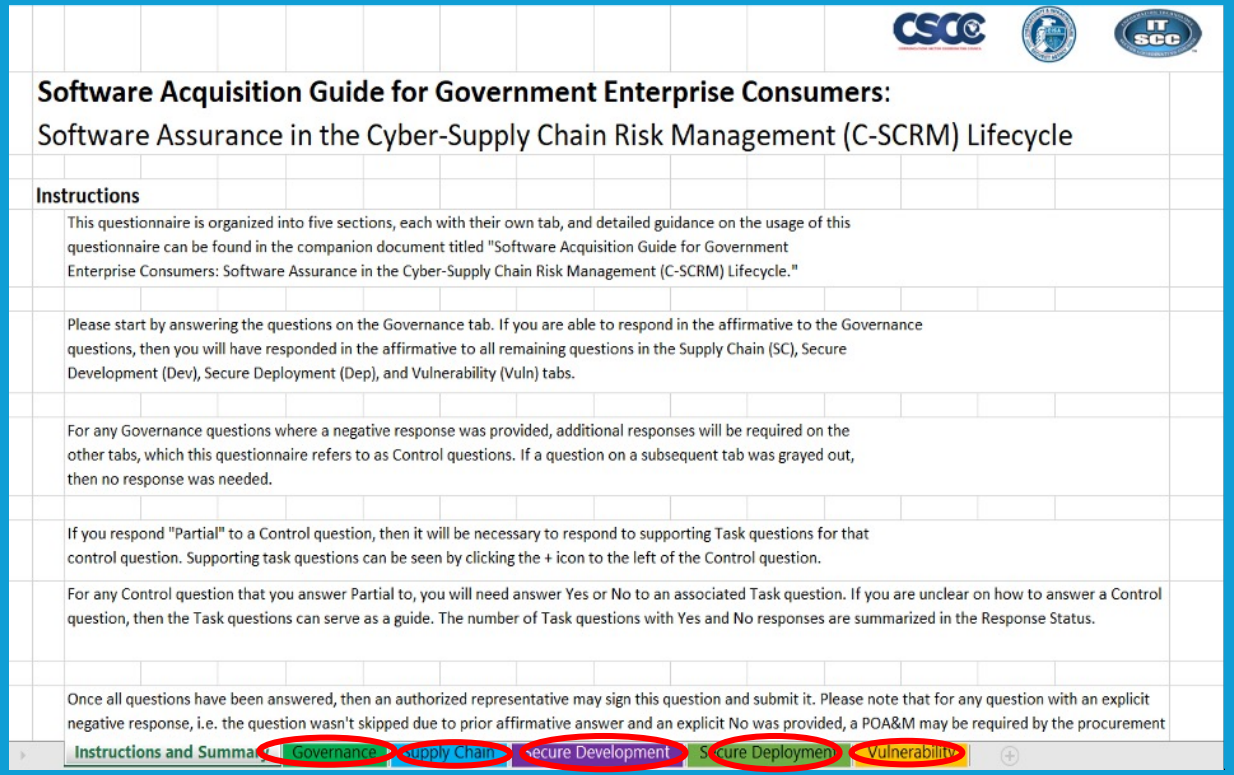
— for Supply Chain: SC.04, SC.07, SC.08
— for Software Development: DEV.03,DEV.07, DEV.08, DEV.09, DEV.10, DEV.11, DEV.12, DEV.14, DEV.20, DEV.21, DEV.22, DEV.23, DEV.26, DEV.27, DEV.28, DEV.30
— for Software Deployment: DEP.07, DEP.09, DEP.11
— for Vulnerability Management: VULN.01, VULN.04, VULN.07

CONTROL.GOV.02 Does the supplier maintain provenance data for internal and third-party components?

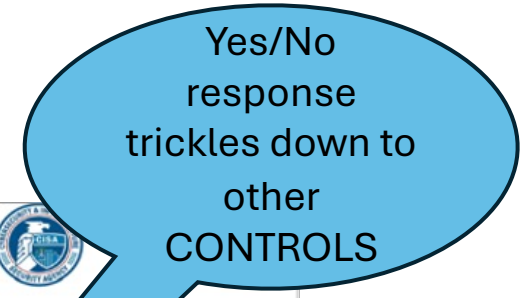
If ‘Yes,’ then the following CONTROL questions and associated TASK questions can be skipped:
— for Supply Chain: SC.01, SC.04, SC.08
— for Software Development: DEV.03, DEV.12, DEV.16, DEV.30

Software Acquisition guide Spreadsheet

- The spreadsheet can be found on the CISA website
- Developed to make the Guide easier to navigate
- Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle | CISA
- An online survey tool is available to key-in responses and export the response data from each sections.



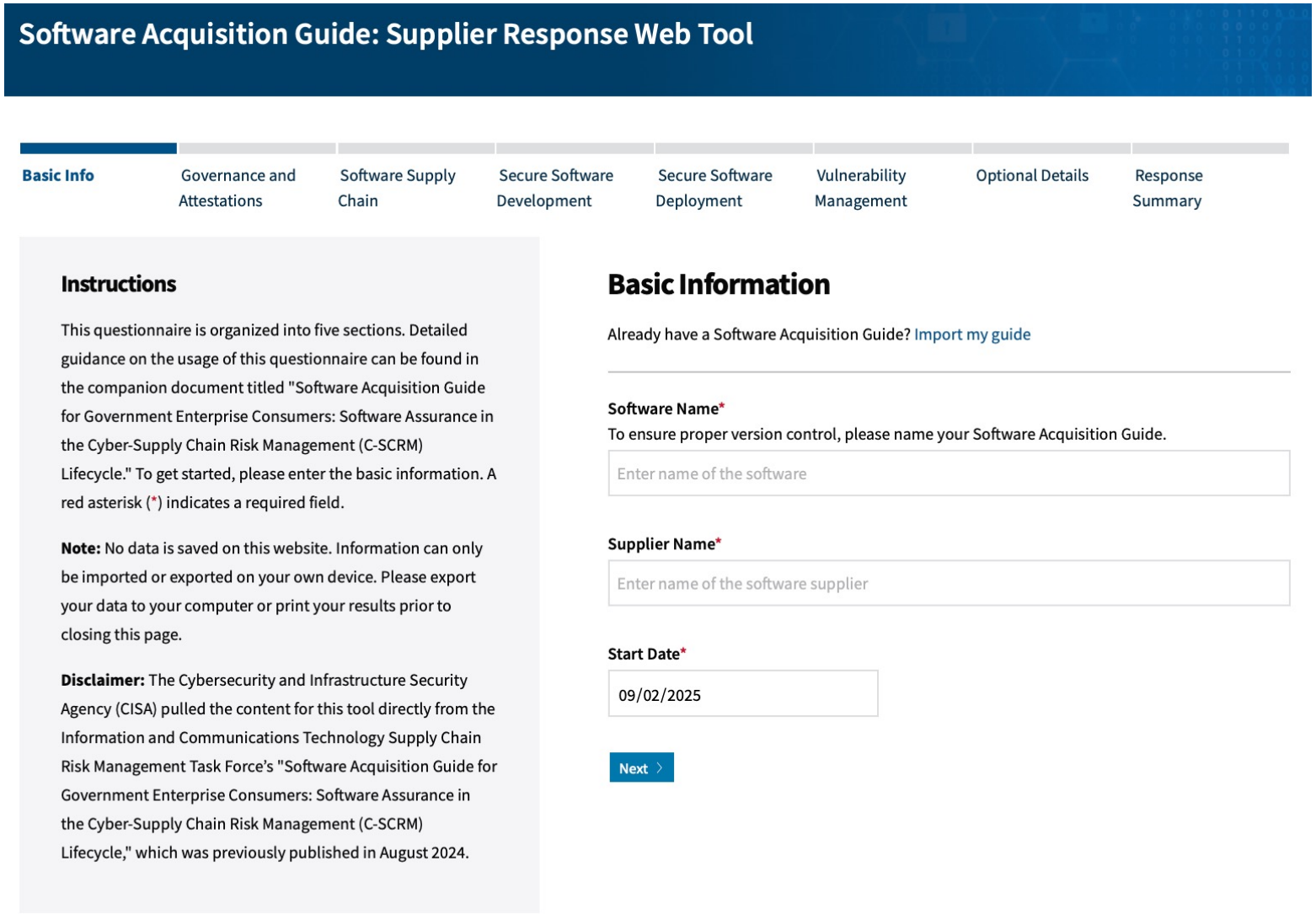
Software Acquisition guide Spreadsheet



Instructions:	Answer the Governance (**GOV**) questions below first to determine whether additional information is needed for the subsequent sections. Use the Answer column to select **Yes** or **No** for each of the 19 questions.		
	The **Estimated Time for Response** represents the experience of sample users.		
Software Acquisition Guide Control Number	**Software Acquisition Guide CONTROL Description**	**Answer**	**Estimated Time for Response**
CONTROL.GOV.01	Does the supplier provide a CISA Secure Software Development Attestation Form, or equivalent such as the GSA 7700 Secure Software Development Attestation Form, without need for a POA&M, signed by the supplier's designated employee (Chief Executive Officer or designee that can bind the supplier)?		ss than 1 minute
CONTROL.GOV.02	Does the Supplier maintain provenance data for internal and third-party components?		Requires research less than 1 hour
CONTROL.GOV.03	Has the supplier's product(s) or product line employed automated tools or comparable processes including, but not limited to, log management and patch management to maintain integrity of software supply chains and to check for and mitigate security-relevant vulnerabilities in binary, source code, development, and build systems?		Requires research less than 1 hour
CONTROL.GOV.04	Has all the software (including third-party and open source) to be delivered undergone rigorous code analysis and multi-level testing according to the supplier's documented testing procedures? Foremost in this testing is the identification of code weaknesses and software vulnerabilities, including those listed in the DHS CISA Known Exploited Vulnerabilities (KEV) Catalog with vulnerable components either patched, rebuilt, or otherwise mitigated.		Requires research less than 1 hour

DEMO: ONLINE SURVEY TOOL

Online Survey Tool



Secure by Design/Demand

- The Software Acquisition Guide focuses on the “Secure by Demand” elements by providing recommendations for procurement and contracting staff, or establishing requirements, to engage in more relevant discussions with their enterprise risk owners and candidate suppliers.
- The Guide enhances an organization’s ability to make risk-informed decisions that are associated with acquisition and procurement of software and cyber-physical products.

- The Secure by Demand Guide compliments the Software Acquisition Guide by assisting organizations acquiring software better understand their software manufacturer’s approach to cybersecurity and ensures that Secure by Design is one of their core considerations.
- Secure by Design Pledge | CISA

HOW NETAPP USES THE SOFTWARE ACQUISITION GUIDE?

NetApp

NetApp Trusted Supplier Program

- To help our supply chain meet the same high standards for security as those enforced within our own organization, NetApp strives to have every one of our suppliers adhere to secure development lifecycle (SDL) best practices through periodic audits and assessments.
- The Trusted Supplier Program is designed to ensure that all third-party suppliers engaged in developing NetApp products have an established, secure development lifecycle process.
    - Suppliers must complete a self-assessment that includes control criteria derived from NIST SP800-161r1upd, NIST SSDF, NIST RMF and Software Acquisition Guide.
- The responses received from suppliers are used to compute an overall risk score for a given supplier and helps to identify specific areas for improvement.
    - All new supplier contracts and contract renewals includes Trusted Supplier Program expectations and compliance requirements.

References

- CISA Software Acquisition Guide and companion artifacts:
  - https://www.cisa.gov/resources-tools/resources/software-acquisition-guide-government-enterprise-consumers-software-assurance-cyber-supply-chain
- Online survey web tool: https://www.cisa.gov/software-acquisition-guide/tool
- CISA Webinar (November 2024):
  - https://www.youtube.com/watch?v=TfguNi5KVdQ
- Presentation in SSCA Forum Spring 2024:
  - https://csrc.nist.gov/Presentations/2024/ict-scrm-task-force-on-swa-buyers-guide

THANK YOU