VENDOR SUPPLY CHAIN RISK MANAGEMENT (SCRM) TEMPLATE

April 2021

This page is intentionally left blank.

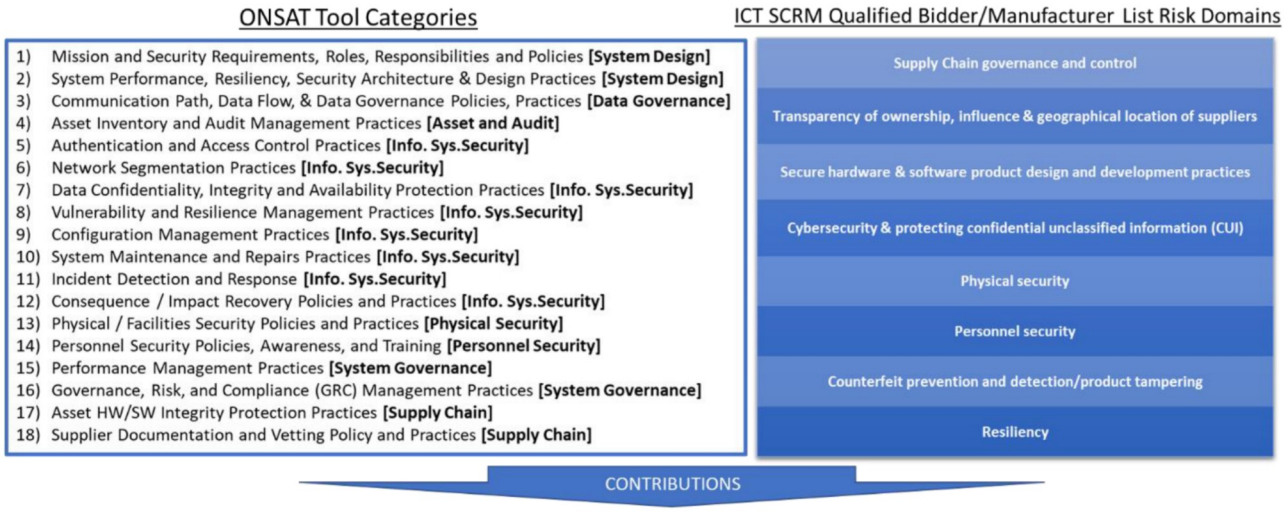
VENDOR SUPPLY CHAIN RISK MANAGEMENT (SCRM) TEMPLATE

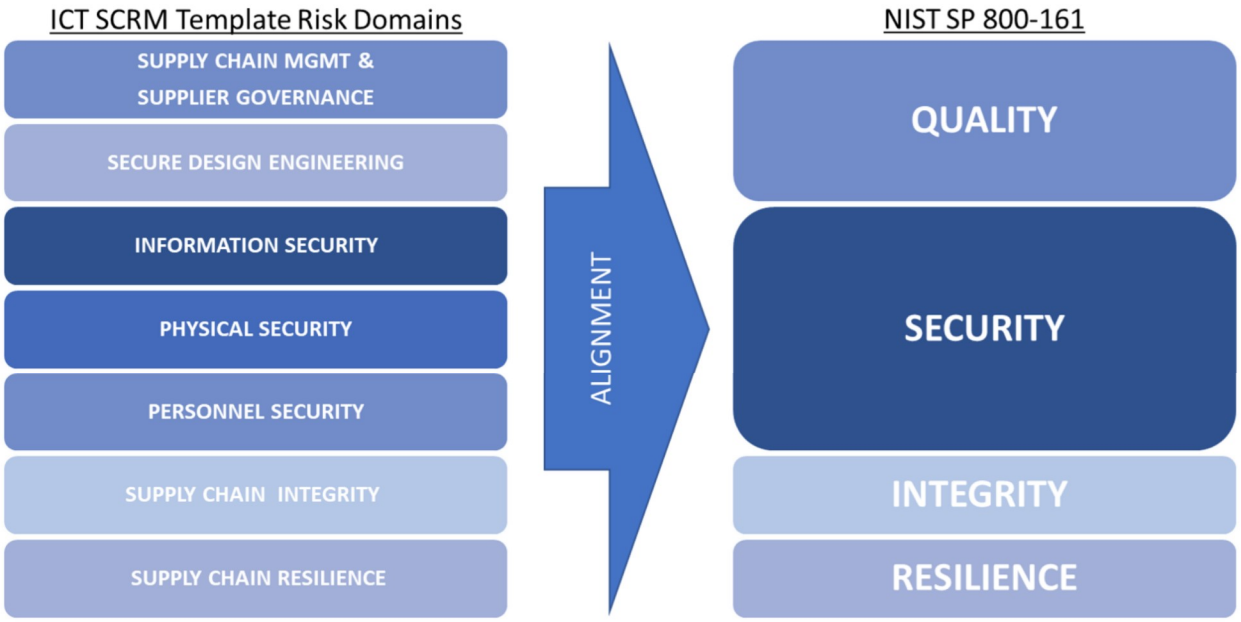
Abstract

The following document is the result of a collaborative effort produced by the Cybersecurity and Infrastructure Security Agency (CISA) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, Working Group 4 (hereinafter WG4), aimed at creating a standardized template of questions as a means to communicate ICT supply chain risk posture in a consistent way among public and private organizations of all sizes. The purpose of this assessment template is to normalize a set of questions regarding an ICT Supplier/Provider implementation and application of industry standards and best practices. This will enable both vendors and customers to communicate in a way that is more consistently understood, predictable, and actionable. These questions provide enhanced visibility and transparency into entity trust and assurance practices and assist in informed decision-making about acceptable risk exposure.

This assessment may be used to illuminate potential gaps in risk management practices and provides a flexible template that can help guide supply chain risk planning in a standard way. It is meant to be non-prescriptive and no specific use case is being mandated. The suggested use is as a tool for consistently analyzing risk when comparing potential new providers. This template builds upon existing industry standards to provide step-by-step guidance and improved awareness Key categories of vendor SCRM compliance are defined within the document, building on a framework of established industry standards and other Task Force efforts, while incorporating inputs from key industry standards and best practices, such as NIST SP 800-161, the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC), and the Outsourcing Network Services Assessment Tool (ONSAT).

The graphics below illustrate the incorporation of ONSAT Tool categories and input from the ICT SCRM Qualified Bidder/Manufacturer Lists (from CISA ICT SCRM Task Force Working Group 3) across the Template categories, as well as alignment of the Template categories to the NIST SP 800-161 categories.


ONSAT Tool Categories
1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]
2) System Performance, Resiliency, Security Architecture & Design Practices [System Design]
3) Communication Path, Data Flow, & Data Governance Policies, Practices [Data Governance]
4) Asset Inventory and Audit Management Practices [Asset and Audit]
5) Authentication and Access Control Practices [Info. Sys.Security]
6) Network Segmentation Practices [Info. Sys.Security]
7) Data Confidentiality, Integrity and Availability Protection Practices [Info. Sys.Security]
8) Vulnerability and Resilience Management Practices [Info. Sys.Security]
9) Configuration Management Practices [Info. Sys.Security]
10) System Maintenance and Repairs Practices [Info. Sys.Security]
11) Incident Detection and Response [Info. Sys.Security]
12) Consequence / Impact Recovery Policies and Practices [Info. Sys.Security]
13) Physical / Facilities Security Policies and Practices [Physical Security]
14) Personnel Security Policies, Awareness, and Training [Personnel Security]
15) Performance Management Practices [System Governance]
16) Governance, Risk, and Compliance (GRC) Management Practices [System Governance]
17) Asset HW/SW Integrity Protection Practices [Supply Chain]
18) Supplier Documentation and Vetting Policy and Practices [Supply Chain]
ICT SCRM Qualified Bidder/Manufacturer List Risk Domains
Supply Chain governance and control
Transparency of ownership, influence & geographical location of suppliers
Secure hardware & software product design and development practices
Cybersecurity & protecting confidential unclassified information (CUI)
Physical security
Personnel security
Counterfeit prevention and detection/product tampering
Resiliency
CONTRIBUTIONS


ICT SCRM Template Risk Domains
SUPPLY CHAIN MGMT & SUPPLIER GOVERNANCE
SECURE DESIGN ENGINEERING
INFORMATION SECURITY
PHYSICAL SECURITY
PERSONNEL SECURITY
SUPPLY CHAIN INTEGRITY
SUPPLY CHAIN RESILIENCE
ALIGNMENT
NIST SP 800-161
QUALITY
SECURITY
INTEGRITY
RESILIENCE

Contents

INTRODUCTION

The questions below broadly cover ICT Supply Chain Risk Management, governance, and associated risk domains. The intent is to illuminate the risk factors that the acquiring organization requires to understand how the risk profile of the entity aligns with their tolerance of risk for the specific product/service being provided. They will aid in mitigating (not eliminating) risk and are consistent with commercial and public sector standards. The questions should be used as applicable, depending on the product/service and the customer involved (*e.g.*, DoD, civilian, commercial).

Recommended Use

- Provide a contact (name, email, and phone number) for questions, support, or additional information related to the questionnaire to the respondents.
- Please provide a response to each 'Yes', 'No' question as relevant to the offering.
- If the question does not apply to your organization, please answer 'N/A' and provide a supporting statement of applicability if not relevant to the offering in consideration.
- A response of 'Alternate' may be used if a particular supply chain risk can be addressed in alternative ways and not directly through compliance with a standard or framework.
- Please attach supporting documents to the completed questionnaire. You may provide links when submitting if documentation is available online and accessible.
- If the respondent(s) is able provide proof of affirmative answers to the initial "bypass questions", the remainder of the assessment is not required.

We recommend designating one primary POC from your organization who will collaborate with the appropriate POCs/teams/vendor/supplier to coordinate and collect and compile responses for each section. The appropriate POCs within each organization will vary and may consist of individuals in acquisition, procurement, supply chain, or security offices. While related, each section is design to be relevant to a different aspect of your organization.

This template is intended to gather an initial and consistent baseline and additional follow-up questions from the organization, or other documentation, may be warranted.

1. QUALIFYING QUESTIONS

If you can provide affirmative responses to the questions below AND supporting, non-expired documentation, you may skip ALL remaining questions.

1.1. Have you previously provided supply chain risk management information to this organization?

If 'Yes,' please provide an updated revision covering material changes.

OR

1.2. Do you have controls fully aligned to NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organization?

1.2.1. Please provide proof of the scope of controls implemented and how controls were validated.

1.2.2. Provide any additional supporting documentation of relevant and current third-party assessments or certification for supply chain risk management, such as ANSI/ASIS SCRM 1.2014, ISO 28000:2007, ISO 31000, ISO 20243, etc.

If you responded affirmatively to ANY of the questions above, you may attach supporting documentation, **skip the remaining questions,** and continue to the signature page.

2. SUPPLY CHAIN MANAGEMENT AND SUPPLIER GOVERNANCE

General

2.1. Do you have policies to ensure timely notification of updated risk management information previously provided to us?

[Yes, No, Alternate, or N/A]

2.1.1. How do you notify us of changes?

2.1.2. What is your customer notification policy?

Information Communications Technology (ICT) Supply Chain Management

2.2. Do you have a documented Quality Management System (QMS) for your ICT supply chain operation based on an industry standard or framework?

[Yes, No, Alternate, or N/A]

2.2.1. Please provide the document which describes your QMS, including any standards or frameworks to which it is aligned.

2.3. Do you have an organization-wide strategy for managing end-to-end supply chain risks (from development, acquisition, life cycle support, and disposal of systems, system components, and to system services)?

[Yes, No, Alternate, or N/A]

2.3.1. What is your strategy?

2.3.2. How have you implemented it?

Authentication and Provenance

2.4. Do you have a policy or process to ensure that none of your suppliers or third-party components are on any banned list?

[Yes, No, Alternate, or N/A]

2.5. Do you provide a bill of materials (BOM) for your products, services, and components which includes all logic-bearing (e.g., readable/writable/programmable) hardware, firmware, and software?

[Yes, No, Alternate, or N/A]

2.5.1. If you provide a BOM that does not include all logic-bearing hardware, firmware, and software, what does your BOM include?

2.5.2. Upon request, are you able to provide your BOM including all logic-bearing hardware, firmware, and software?

2.5.3. How do you track changes in your products, services, and components and how do you reflect those changes in the applicable BOM(s)?

2.6. For hardware components included in the product offering, do you only buy from original equipment manufacturers or licensed resellers?

[Yes, No, Alternate, or N/A]

2.7. Do you have a process for tracking and tracing your product while in development and manufacturing?

[Yes, No, Alternate, or N/A]

2.7.1. How do you keep track of your chain of custody?

2.7.2. How do you track and trace components within your product?

Supplier Governance

2.8. Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers?

[Yes, No, Alternate, or N/A]

2.8.1. What are your SCRM requirements?

2.8.2. How do you verify that your suppliers are meeting contractual terms and conditions, which may include requirements to be passed down to sub-suppliers?

2.8.3. If violations of contractual SCRM requirements or SCRM-related incidents occur, do you ensure and monitor any remediation activities?

2.9. Do you revise your written SCRM requirements regularly to include needed provisions?

2.10. Do you have policies for your suppliers to notify you when there are changes to their subcontractors or their offerings (components, products, services, or support activities)?

[Yes, No, Alternate, or N/A]

2.10.1. Please describe your policy.

3. SECURE DESIGN AND ENGINEERING

Note: If your answer to the question below is 'Yes,' please continue and complete the remaining questions in this section. If your answer is 'No,' you may skip the remainder of this section and move on to the next section of this questionnaire.

3.1. Does your organization develop (or integrate) custom hardware or software offerings?

[Yes, No, Alternative]

3.1.1. List the custom software, hardware, system, or solution offering(s) provided by your organization.

Product Offering Lifecycle Management and Organization

3.2. Do you implement formal organizational roles and governance responsible for the implementation and oversight of Secure Engineering across the development or manufacturing process for product offerings?

[Yes, No, Alternate, or N/A]

3.2.1. If so, how are roles, responsibilities, and practices validated?

3.3. What security control framework (industry or customized) is used to define product offering security capabilities?

Please describe or 'N/A'

3.4. Does your organization document and communicate security control requirements for your hardware, software, or solution offering?

[Yes, No, Alternate, or N/A]

3.4.1. How are security requirements validated as part of the product offering development or manufacturing process?

3.5. How does your organization implement development and manufacturing automation to enforce lifecycle processes and practices?

Protect IP and Product (Supplier) Offering Assets

3.6. Does your organization protect all forms of code from unauthorized access and tampering, including patch updates?

[Yes, No, Alternate, or N/A]

3.6.1. How does your organization prevent unauthorized changes to code, both

inadvertent and intentional, which could circumvent or negate the intended security characteristics of the software?

3.7. Does your organization provide a mechanism for verifying software release integrity, including patch updates for your software product offering?

[Yes, No, Alternate, or N/A]

3.8. How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution?

3.9. Does your organization manage the integrity of IP for its product offering?

[Yes, No, Alternate, or N/A]

3.9.1. How does your organization archive assets associated with the product offering development or manufacturing process?

Secure Coding and Manufacturing Practices

3.10. Does your organization define, follow, and validate secure coding and manufacturing practices to mitigate security risks?

[Yes, No, Alternate, or N/A]

3.10.1. How does your organization conduct threat modeling to determine required product offering security requirements?

3.10.2. How does your organization determine how identified risks are mitigated in product offering design?

3.10.3. How does your organization justify risk-based decisions to relax or waive security requirements or controls?

3.10.4. How does your organization validate that the offering will meet the security requirements and satisfactorily address the identified threat assessment?

3.11. Does your organization verify that third-party software provides required security requirements/controls?

[Yes, No, Alternate, or N/A]

3.11.1. How does your organization reduce the risk associated with using acquired software modules and services, which are potential sources of additional vulnerabilities?

3.12. Does your organization reuse existing, well-secured software and hardware components, when feasible, instead of duplicating functionality?

[Yes, No, Alternate, or N/A]

3.13. Does your organization configure the compilation and build processes to improve executable security?

[Yes, No, Alternate, or N/A]

3.13.1. How does your organization decrease the number of security vulnerabilities in the software and reduce costs by eliminating vulnerabilities before testing occurs?

3.14. Does your organization implement formal vulnerability and weakness analysis practices?

[Yes, No, Alternate, or N/A]

3.14.1. Does your organization automate the identification of security vulnerabilities and weaknesses?

3.14.2. Does your organization test executable code or components to identify vulnerabilities and verify compliance with security requirements?

3.15. Does your organization configure offerings to implement secure settings by default?

[Yes, No, Alternate, or N/A]

3.15.1. Does your organization test offerings using hardened runtime environments?

Respond to Vulnerabilities (RV)

3.16. Does your organization maintain and manage a Product Security Incident Reporting and Response program (PSRT)?

[Yes, No, Alternate, or N/A]

3.16.1. How does your organization assess, prioritize, and remediate reported vulnerabilities?

3.16.2. How does your organization ensure that vulnerabilities are remediated in a timely period, reducing the window of opportunity for attackers?

3.17. Does your organization analyze vulnerabilities to identify root cause?

[Yes, No, Alternate, or N/A]

3.17.1. Are vulnerability root causes used as input to update secure development process, tools, and training to lower future vulnerabilities?

4. INFORMATION SECURITY

4.1. Do you hold a valid information security/cybersecurity third-party attestation or certification? (e.g., ISO 27001, SOC 2 Type 2, CMMC Level 3-5, Cybersecurity Maturity Assessment, etc.)

[If yes, please state the program and date that you were certified, and provide a copy of the certification. You may skip the remaining questions of this section and proceed to the following section. If no, continue.]

4.2. Do you follow operational standards or frameworks for managing Information Security/Cyber security? (e.g., NIST CSF 1.1, NIST 800-37, Rev. 2, NIST SP 800-161, ISO IEC 27001, ISO 20243, ISO 27036, SAE AS649)

[Yes, No, Alternate, or N/A]

4.2.1. If so, please state which one(s)?

4.3. Do you have company-wide, publicly available information security policies in place covering privacy policies?

[Yes, No, Alternate, or N/A]

4.3.1. If 'Yes', please provide.

4.3.2. What mechanisms are in place to ensure your policies are enforced within your supply chain?

4.3.2.1. Do you receive notification of and have a response plan in place for privacy violations of the suppliers in your supply chain?

Asset Management

4.4. Do you inventory and audit back-up and/or replacement hardware and software assets to ensure their accountability and integrity?

[Yes, No, Alternate, or N/A]

4.4.1. What recognized standards or frameworks do you follow to ensure integrity of back-up assets? (e.g., NIST 800-53, NIST 800- 171 DFARS, ISA/IEC 62443 or ISO 27001/2)

4.5. Do you have a defined governance scope for asset management, including line of business technology, facilities, devices, and all other data- generating hardware (like Internet of Things devices)?

[Yes, No, Alternate, or N/A]

4.6. Do you have processes or procedures in place to ensure that devices and software installed by users external to your IT department (e.g., line of business personnel) are being discovered, properly secured, and managed?

[Yes, No, Alternate, or N/A]

4.6.1. What, if any, types of assets are out of scope for your tracking procedures?

4.7. Do you have an asset management program approved by management for your IT assets that is regularly maintained?

[Yes, No, Alternate, or N/A]

4.7.1. What are your methods to manage IT assets on the network?

4.7.1.1. How do you manage other IT hardware and software assets which are not network connected, regardless of network presence?

4.7.2. What are your methods of verifying acceptable use of assets, including verified asset return, for your network-connected assets?

4.8. Do you have documented policies or procedures to manage enterprise network-connectable assets throughout their lifecycle?

[Yes, No, Alternate, or N/A]

4.8.1. What are your processes to manage obsolescence of network-connected assets?

4.8.2. What are your policies or procedures to ensure your enterprise software platforms and applications, and hardware assets, are classified according to their criticality?

4.8.3. What are your policies or procedures to ensure appropriate controls are in place for internal or third-party cloud services?

4.9. Do you ensure that you are not sourcing assets on a banned list to customers (e.g., ITAR, NDAA Section 889)?

[Yes, No, Alternate, or N/A]

4.9.1. How do you ensure that you are not providing assets on a banned list to customers?

4.10. Do you have documented hardware and software policies and practices in place to ensure asset integrity?

[Yes, No, Alternate, or N/A]

4.10.1. What recognized standards or frameworks are followed to ensure asset integrity?

4.10.1.1. How do you ensure that regular reviews and updates of the asset integrity policies and practices are performed?

Identify

4.11. Do you have documented policies or procedures for identification and detection of cyber threats?

[Yes, No, Alternate, or N/A]

4.11.1. What processes do you have in place to promptly detect cyber threats?

4.11.1.1. How do you manage the identification of threats within your supply chain, including suppliers and sub-contractors?

4.11.1.2. What processes are in place to act upon external credible cyber security threat information received?

4.12. Do you address the interaction of cybersecurity operational elements (e.g., SOC, CSIRT, etc.) with the physical security operational elements protecting the organization's physical assets?

[Yes, No, Alternate, or N/A]

4.12.1. How do you ensure that physical security incidents and suspicious events are escalated to cybersecurity operations staff?

4.12.2. Are cybersecurity vulnerabilities for industrial control systems, including physical access controls and video monitoring systems, tracked?

4.12.3. What standards or frameworks are followed for management of IT and OT system interactions?

4.13. Do you have a policy or procedure for the handling of information that is consistent with its classification?

[Yes, No, Alternate, or N/A]

4.13.1. What is your process to verify that information is classified according to legal, regulatory, or internal sensitivity requirements?

4.13.1.1. How do you convey requirements for data retention, destruction, and encryption to your suppliers?

4.14. Do you have documented policies or procedures for internal identification and management of vulnerabilities within your networks and enterprise systems?

[Yes, No, Alternate, or N/A]

4.14.1. What industry standards or frameworks are followed for vulnerability management

4.14.1.1. How do you identify vulnerabilities in your supply chain (suppliers/sub-contractors) before they pose a risk to your organization?

4.14.1.2. How do you assess and prioritize the mitigation of vulnerabilities discovered on your internal networks and systems? (e.g., asset criticality, exploitability, severity, etc.)

Protect

4.15. Do you have network access control policies and procedures in place for your information systems that are aligned with industry standards or control frameworks?

[Yes, No, Alternate, or N/A]

4.15.1. If Yes, please list any standards or frameworks used.

4.15.2. What are your practices for items such as federation, privileged users, and role-based access control for end-user devices?

4.15.2.1. How do you ensure remote access is managed for end-user devices or employees and suppliers, including deactivation of accounts? (e.g. Multi-factor authorization, encryption, protection from malware, etc.)

4.15.2.2. How do you identify and correct end-user systems that fall out of compliance?

4.16. Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?

[Yes, No, Alternate, or N/A]

4.16.1. What is the frequency for verifying personnel training compliance?

4.16.2. What cybersecurity training is required for your third-party stakeholders (e.g., suppliers, customers, partners, etc.) who have network access?

4.16.2.1. How is training compliance tracked for third parties with network access?

4.17. Do you include contractual obligations to protect information and information systems handled by your suppliers?

[Yes, No, Alternate, or N/A]

4.17.1. What standard cybersecurity standards or frameworks are the contractual supplier terms for information protection aligned to, if any?

4.18. Do you have an organizational policy on the use of encryption that conforms with industry standards or control frameworks?

[Yes, No, Alternate, or N/A]

4.18.1. What industry standards or controls frameworks are followed for encryption and key management?

4.18.2. What processes or procedures exist to comprehensively manage the use of encryption keys?

4.18.2.1. What is your process for protecting data at rest and in transit?

4.19. Does your organization have hardening standards in place for network devices (e.g., wireless access points, firewalls, etc.)?

[Yes, No, Alternate, or N/A]

4.19.1. What protections exist to provide network segregation where appropriate (e.g., intrusion detection systems)?

4.19.2. What controls exist to continuously monitor changes to your network architecture (e.g., NIST 800-53 or related controls)?

4.19.3. How do you manage prioritization and mitigation of threats discovered on your networks?

4.19.4. How do you track changes to software versions on your servers?

4.20. Do you follow an industry standard or framework for your internal or third- party cloud deployments, if applicable?

[Yes, No, Alternate, or N/A]

4.20.1. What protections are in place between your network and cloud service providers?

4.20.1.1. How to do you convey cloud security requirements to your suppliers/sub-contractors?

Detect

4.21. Do you have defined and documented incident detection practices that outline which actions should be taken in the case of an information security or cybersecurity event?

[Yes, No, Alternate, or N/A]

4.21.1. Are cybersecurity events centrally logged, tracked, and continuously monitored?

4.21.2. Are incident detection practices continuously improved?

4.22. Do you require vulnerability scanning of software running within your enterprise prior to acceptance?

[Yes, No, Alternate, or N/A]

4.22.1. What procedures or policies exist, if any, for detecting vulnerabilities in externally obtained software (such as penetration testing of enterprise and non-enterprise software)?

4.22.2. What are your procedures to scan for vulnerabilities in supplier-provided software running on your network?

4.23. Do you manage updates, version tracking of new releases, and patches (including patching history) for your software and software services offerings?

[Yes, No, Alternate, or N/A]

4.23.1. What is the responsibility of the product end-user (customer) for updating software versions?

4.24. Do you deploy anti-malware software?

[Yes, No, Alternate, or N/A]

4.24.1. What systems are out of scope for anti-malware software compliance, if any?

4.24.1.1. How do you ensure anti-malware is present on developer platforms? As applicable to your offering?

Respond & Recover

4.25. Do you have a documented incident response process and a dedicated incident response team (CSIRT - Computer Security Incident Response Team)?

[Yes, No, Alternate, or N/A]

4.25.1. What is your process for reviewing and exercising your resiliency plan?

4.25.2. What is your process to ensure customers and external entities (such as government agencies) are notified of an incident when their product or service is impacted?

4.26. Do you have processes or procedures to recover full functionality, including integrity verification, following a major cybersecurity incident?

[Yes, No, Alternate, or N/A]

4.26.1. What is the frequency for testing of back-up media?

4.27. Do you insure for financial harm from a major cybersecurity incident (e.g., self-insure, third-party, parent company, etc.)?

[Yes, No, Alternate, or N/A]

4.27.1. Does coverage include financial harm to your customers resulting from a cybersecurity breach which has impacted your company?

5. PHYSICAL SECURITY

5.1. Is the entity (organization, operational unit, facility, etc.) currently covered by an unrestricted/unlimited National Industrial Security Program (NISP) Facility Clearance (FCL) or a related U.S. government program such as C- TPAT that certifies the entity as meeting appropriate physical security standards?

[If 'Yes,' please state the program that certified you and date of last certification. You may skip the remaining questions of this section and proceed to the next section. If not, continue with this section.]

5.1.1. If the entity is not covered by a NISP FCL but currently has some other US Government or industry attestation, such as TAPA FSR of meeting a physical security code or standard, please identify the standard, the issuing agency, and the most recent date of certification.

5.1.2. Is the entity covered by a limited FCL (in agreement with a foreign government)? Describe.

5.2. Do you have documented security policies and procedures that address the control of physical access to cyber assets (network devices, data facilities, patch panels, industrial control systems, programmable logic, etc.)?

[Yes, No, Alternate, or N/A]

5.2.1. To what standards/controls do you adhere? (e.g., NIST publication, ISO, UL, etc.)

5.2.1.1. How often do you review and update to those policies and procedures and what is the most recent review?

5.2.1.2. If needed, can you provide these documents for our review?

5.3. Do you have documented policies addressing staff training which includes procedures to limit physical access to cyber assets to only those with demonstrated need?

[Yes, No, Alternate, or N/A]

5.3.1. What training do all staff receive to address potential physical security threats and how to respond to emergencies (e.g., fire, weather, etc.)?

5.3.2. What training do cybersecurity staff, physical security staff, and contractors with at least limited access to sensitive areas of a facility receive?

5.3.2.1. How does this training address potential threats to the facility and how the physical access controls are integrated with system network interfaces?

5.3.3. What standards do you follow, or did you implement (e.g., NIST publication, ISO, UL, etc.)?

5.3.3.1. How is this training documented?

5.4. Do you have a documented Security Incident Response process covering physical security incidents? (e.g., potential intruder access, missing equipment, etc.)

[Yes, No, Alternate, or N/A]

5.4.1. What processes do you have in place to document the actions taken during and after an actual or suspected physical security incidents (e.g., security log, formal report to management, police report, etc.)?

5.4.1.1. How do you ensure that your staff understands and complies with procedures (e.g., training, exercises, and actual cases of incident response)?

5.5. For facilities that use an independent contractor for physical security, are physical facilities security policy and procedures incorporated into service level agreements, contracts, policies, regulatory practices?

[Yes, No, Alternate, or N/A]

5.5.1. What physical / facilities security policies and practices are subject to audit?

5.5.2. For contractors who have access to a critical facility, sensitive assets, or major physical plant systems, what standards are they required to attest to? (e.g., NIST publication, ISO, UL, etc.)

5.5.2.1. How is compliance with these standards validated?

5.6. Are there enforcement mechanisms (e.g., sanctions, response procedures, technology) for unauthorized physical access to mission/business critical information, functions, services and assets?

[Yes, No, Alternate, or N/A]

5.6.1. What type of action or response would be taken for unauthorized physical access to sensitive cyber assets?

5.7. Do you have evidence that physical security mechanisms are effective and adequate to protect assets? Evidence could include third-party assessment, self-assessment, records of actions taken to enforce rules, etc.

[Yes, No, Alternate, or N/A]

5.7.1. What is the date of the last review and update to your enforcement strategy?

Physical Security In-transit

5.8. Do you utilize a controlled bill of materials (BOM) or similar capability to protect assets that are being received, in process, or in-transit?

[Yes, No, Alternate, or N/A]

5.8.1. What industry standards or frameworks are followed?

5.9. Do you have requirements that all items being shipped have tamper-evident packaging?

[Yes, No, Alternate, or N/A]

5.9.1. What industry standards or frameworks are being followed to ensure packaging is tamper-evident?

5.9.1.1. How are these requirements audited to ensure that they are effective?

5.10. Do you have processes in place to prevent counterfeit parts from entering your supply chain?

[Yes, No, Alternate, or N/A]

5.10.1. What requirements, if any, are in place to ensure the use of Original Equipment Manufacturer (OEM) or Authorized Distributors for all key components?

5.10.2. What are your processes for the detection and disposition of counterfeit electronic components?

5.10.2.1. How do you pass on counterfeit prevention requirements to your third-party suppliers?

6. PERSONNEL SECURITY

6.1. Does a formal personnel security program exist?

[Yes, No, Alternate, or N/A]

6.1.1. Is employee access managed by role?

6.1.2. Is access to business-critical systems, manufacturing facilities, and assets formally managed and maintained? Please describe.

6.1.3. Are physical security practices formally governed, documented, maintained, and enforced?

Onboarding

6.2. Do you have a process for onboarding personnel?

[Yes, No, Alternate, or N/A]

6.2.1. Does the process include security awareness training?

6.2.2. What is the process to determine the level of access to company identifications (IDs), tokens, documents, applications, etc.?

6.2.3. What is the process to distribute company assets?

6.2.4. Is the onboarding process documented?

6.2.4.1. If 'Yes', please provide a copy.

6.3. Do you have policies for conducting background checks of your employees as permitted by the country in which you operate?

[Yes, No, Alternate, or N/A]

6.3.1. If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.

6.3.2. How do you conduct the background checks and document, validate, and update their responses?

6.4. Do you have policies for conducting background checks for your suppliers, as permitted by the country in which you operate?

[Yes, No, Alternate, or N/A]

6.4.1. If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.

6.4.2. How do you conduct the background checks and document, validate, and update their responses?

6.5. Do you have policies for conducting background checks for any subcontractors, as permitted by the country in which you operate?

[Yes, No, Alternate, or N/A]

6.5.1. If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.

6.5.2. How do you conduct the background checks and document, validate, and update their responses?

Offboarding

6.6. Do you have a process for offboarding personnel?

[Yes, No, Alternate, or N/A]

6.6.1. Does the process include a process to transfer knowledge to other personnel?

6.6.2. What is the process to remove access to all company documents, applications, assets, etc.?

6.6.3. What is the process to recover all company assets?

6.6.4. Is that process documented?

Awareness and Training (Security-Specific)

6.7. Are personnel security practices formally documented and accessible to all employees?

[Yes, No, Alternate, or N/A]

6.8. Are Personnel Security practices routinely enforced, audited, and updated?

[Yes, No, Alternate, or N/A]

6.9. Are personnel required to complete formal SCRM training annually?

[Yes, No, Alternate, or N/A]

6.10. Are all personnel trained in security best practices? This includes, but is not limited to, insider threats, access control, and data protection.

[Yes, No, Alternate, or N/A]

6.11. Is there additional security training provided to users with elevated privileges?

[Yes, No, Alternate, or N/A]

6.12. Are you aware of security training practices performed by your sub-suppliers to their personnel?

[Yes, No, Alternate, or N/A]

6.12.1. If 'Yes', does it align with your security practices?

6.13. Do you have a Code of Conduct for your employees, suppliers and subcontractors?

[Yes, No, Alternate, or N/A]

6.13.1. Is the Code of Conduct always available and visible to your employees, suppliers, and subcontractors?

6.13.2. How [regularly or often] is this Code of Conduct updated? Please describe the frequency.

6.13.3. Do you have personnel designated to address questions or violations to the Code of Conduct?

6.13.4. Are these employees, suppliers, and subcontractors trained on the Code of Conduct, including privacy and confidentiality requirements, as required by your industry?

7. SUPPLY CHAIN INTEGRITY

7.1. Do your processes for product integrity conform to any of the following standards (e.g., ISO 27036, SAE AS6171, etc.)?

[Yes, No, Alternate, or N/A]

7.2. Do you control the integrity of your hardware/software (HW/SW) development practices by using Secure Development Lifecycle practices?

[Yes, No, Alternate, or N/A]

7.2.1. How do you manage the conformance of your third parties to your procedures?

7.3. Do you have documented performance and validation procedures for your HW/SW products or services?

[Yes, No, Alternate, or N/A]

7.3.1. What is your process to ensure conformance to those procedures?

7.3.1.1. How do you manage HW/SW products or service that are not in compliance with those procedures?

7.3.1.2. How are subcontractors held accountable to performance specifications?

7.3.2. What, if any, automated controls are in place for your validation processes?

7.3.2.1. How do you audit your validation processes?

7.4. Do you have processes in place to independently detect anomalous behavior and defects in HW/SW products or services?

[Yes, No, Alternate, or N/A]

7.4.1. What means do you provide to allow customers to report anomalies?

7.4.1.1. How do you monitor and track anomalous product or service behavior?

7.5. Do you monitor third-party HW/SW products or services for defects?

[Yes, No, Alternate, or N/A]

7.5.1. What are your processes for managing third-party products and component defects throughout their lifecycle?

7.6. Does the functional integrity of your product or services rely on cloud services (commercial or hybrid)?

[Yes, No, Alternate, or N/A]

7.6.1. What policies and procedures are in place to protect the integrity of the data provided through cloud services?

7.6.1.1. How do you manage the shared responsibility for cloud service integrity requirements with your suppliers?

7.7. Do you have required training on quality and product integrity processes for employees, suppliers, and subcontractors?

[Yes, No, Alternate, or N/A]

7.7.1. What mechanisms are in place for direct employees and contracted workers to ensure applicable training has been completed?

7.7.1.1. Do you pass down training requirements to your sub-suppliers, as applicable?

7.8. Do you have processes to evaluate prospective third-party suppliers' product integrity during initial selection?

[Yes, No, Alternate, or N/A]

7.8.1. What processes or procedures, if any, are in place to ensure that prospective suppliers have met your product integrity requirements?

7.8.1.1. How do your policies or procedures ensure appropriate management/leadership input on supplier selection decisions?

7.9. Do you have regularly scheduled audits to ensure compliance with HW/SW products or services integrity requirements?

[Yes, No, Alternate, or N/A]

7.9.1. What provisions for auditing are included within supplier contracts?

7.9.2. How do you pass down HW/SW products or services integrity requirements to third-party suppliers?

7.10. Do you have a process for improving integrity of HW/SW products or services?

[Yes, No, Alternate, or N/A]

7.10.1. What programs are in place to ensure continuous performance monitoring and improvement of key suppliers?

7.11. Do you have processes in place for addressing reuse and/or recycle of HW products?

[Yes, No, Alternate, or N/A]

7.11.1. What is your process?

8. SUPPLY CHAIN RESILIENCE

General

8.1. Does your organization have a formal process for ensuring supply chain resilience as part of your product offering SCRM practices?

[Yes, No, Alternate, or N/A]

8.1.1. What standards or industry frameworks do you use to help inform those practices?

8.2. Do you consider non-technical supply chain resilience threats such as weather, geo-political instability, epidemic outbreak, volcanic, earthquakes, etc.?

Supply Chain Disruption Risk Management (Business Continuity)

8.3. Do you maintain a formal business continuity plan necessary to maintain operations through disruptions and significant loss of staff?

[Yes, No, Alternate, or N/A]

8.3.1. If illness causes high absenteeism, are personnel cross-trained and able to perform multiple duties?

8.4. Do you maintain a formally trained and dedicated crisis management team, including on-call staff, assigned to address catastrophic or systemic risks to your supply chain or manufacturing processes?

[Yes, No, Alternate, or N/A]

8.4.1. Do you require and audit key suppliers for their ability to be prepared for unexpected supply chain disruptions?

8.5. Can personnel work remotely?

[Yes, No, Alternate, or N/A]

8.5.1. Do your service deliverables outline which services can be done remotely and which cannot?

8.5.1.1. Is that documented in Service-level agreement (SLA) or Terms and Conditions?

8.5.1.2. What infrastructure support is needed to support a shift to an at-home workforce?

Diversity of Supply Base

8.6. Does your company consider supplier diversity to avoid single sources and to reduce the occurrence of suppliers being susceptible to the same threats to resilience?

[Yes, No, Alternate, or N/A]

8.7. Does your company consider alternate offering delivery channels to mitigate extended supplier outages to include cloud, network, telecommunication, transportation, and packaging?

[Yes, No, Alternate, or N/A]

SIGNATURES:

Please include the names and titles of all persons completing this template.

Name: Date:

Title:

Signature: X_____

Name: Date:

Title:

Signature: X_____

Name: Date:

Title:

Signature: X_____

Name: Date:

Title:

Signature: X_____

Name: Date:

Title:

Signature: X_____

APPENDIX A: REFERENCE MATERIALS

Qualifying Questions

Question 1.1

- NIST SP 800-53 (SA-12; SA-12 (1); SA-12 (2); SA (12(14); SA-11
- NIST IR 7622

Question 1.2

- NIST SP 800-161, ANSI/ASIS SCRM 1.2014, ISO 28000:2007, ISO 31000

SUPPLY CHAIN MANAGEMENT & SUPPLIER GOVERNANCE

Questions 2.2, 2.3

- ISO 9001:2015; NIST SP 800-161

Question 2.4

- FY19 NDAA Section 889 Prohibitions, U.S. Executive Order on Securing the Information and Communications Technology and Services Supply Chain 5/15/2019

Question 2.5

- NIST SP 800-161: PV-2; SA-12(13); NIST SP 800-53 (PV-2; SA-12(13))

Questions 2.6, 2.7

- NIST SP 800-53 (rev.4) (SA-12(1) Acquisition Strategies. Questions 1.13 - 1.19.1
- NIST SP 800-161 (SA-3): NIST SP 800-161, Chapter 2, page 21

Questions 2.8, 2.9

- NIST SP 800-53; NIST IR 7622; SIG LITE 2020; ISO 8.4; NIST SP 800-161 (IR-

SECURE DESIGN & ENGINEERING

Question 3.1

- N/A

Questions 3.2, 3.3

- BSIMM10: CP1.1, CP1.3, SR1.1, CP3.2, SM1.1, SM1.2, SM1.3, CP2.5, T1.1, T1.5, T1.7, T2.6, T2.8, T3.2, T3.4
- BSA: SC.1-1, SC.2, PD.1-1, PD.1-2, PD.1-3, PD.2-1, PD.2-2
- ISO 27034: 7.3.2
- MSSDL: Practice 1 & 2
- NISTCSF: ID.GV-3
- OWASPTEST: Phase 2.1
- PCISSLRAP: 1.1, 1.2, 1.3, 2.1

- SAMM15: PC1-A, PC1-B, PC2-A, SR1-A, SR1-B, SR2-B
- SCFPSSD: Planning the Implementation and Deployment of Secure Development Practices; Establish Coding Standards and Conventions
- SCAGILE: Operational Security Tasks 14, 15; Tasks Requiring the Help of Security Experts 1
- NIST SP 800- 53: SA-3, SA-8, SA-15
- NIST SP 800-160: 3.1.2, 3.2.4, 3.3.1, 3.4.2, 3.4.3
- NIST SP 800-181: T0414; K0003, K0039, K0044, K0157, K0168, K0177, K0211, K0260, K0261, K0262, K0524; S0010, S0357, S0368; A0033, A0123, A0151, T0001, T0004
- NISTCSF: ID.AM-6, ID.GV-2
- NISTCSF: PR.AT-*
- SP800160: 3.2.1, 3.2.4, 3.3.1
- SP800181: K0233
- SP800181: OV-TEA-001, OV-TEA-002; T0030, T0073, T0320; K0204, K0208, K0220, K0226, K0243, K0245, K0252; S0100, S0101; A0004, A0057
- SCSIC: Vendor Software Development Integrity Controls
- SAMM15: EG1-A, EG2-A, SM1.A

Question 3.4

- BSA: TV.2-1, TV.5-1, PD1-6
- BSIMM10: SM1.4, SM2.2
- ISO 27034: 7.3.5
- MSSDL: Practice 3
- OWASPTEST: Phase 1.3
- SAMM15: DR3-B, IR3-B, PC3-A, ST3-B
- NIST SP800-53: SA-15
- NIST SP800-160: 3.2.1, 3.2.5, 3.3.1, 3.3.7
- NIST SP800-181: K0153, K0165, T0349; K0153

Question 3.5

- BSA: TC.1, TC.1-1, TC.1-2, TC.1-6, PD.1.6
- MSSDL: Practice 8
- NIST SP800-53: SA-15
- NIST SP800-181: K0013, K00139, K0178
- SCAGILE: Tasks Requiring the Help of Security Experts 9
- SCAGILE: Tasks Requiring the Help of Security Experts 9
- PCISSLRAP: 2.5
- SCAGILE: Tasks Requiring the Help of Security Experts 9

Question 3.6

- BSA: IA.1, IA.2-2, SM.4-1
- IDASOAR: Fact Sheet 25
- NISTCSF: PR.AC-4
- OWASPASVS: 1.10, 10.3.2, 14.2
- PCISSLRAP: 6.1
- SCSIC: Vendor Software Delivery Integrity Controls, Vendor Software Development Integrity Controls

Question 3.7

- BSA: SM.4.2, SM.4.3, SM.5.1, SM.6.1
- BSIMM10: SE2.4
- NISTCSF: PR.DS-6
- PCISSLRAP: 6.2
- SAMM15: OE3-B
- SCSIC: Vendor Software Delivery Integrity Controls
- SP800181: K0178

Question 3.8

- IEC:IECEE, IECQ
- ISO 28000
- ISO 12931
- ISO 16678

Question 3.9

- BSA: PD.1-6,
- PD.1-5, TV.2, TV.3
- BSIMM10: CR1.2, CR1.4, CR1.6, CR2.6, CR2.7
- IDASOAR: Fact Sheets 3, 4, 5, 14, 15, 25, 48
- ISO 27034: 7.3.6
- MSSDL: Practices 9, 10
- NIST CSF: PR.IP-4
- NIST SP 800-53: SA-11, SA-15
- NIST SP 800-181: SP-DEV-002; K0013, K0039, K0070, K0153, K0165; S0174, SP-DEV-001, SP-DEV-002; T0013, T0111, T0176, T0267, T0516; K0009, K0039, K0070, K0140, K0624; S0019, S0060, S0078, S0137, S0149, S0167, S0174, S0242, S0266; A0007, A0015, A0036, A0044, A0047
- OWASPASVS: 1.1.7, 10
- OWASPTEST: Phase 3.2, Phase 4.1
- PCISSLRAP: 4.1, 5.2, 6.2

- SAMM15: IR1-B, IR2-A, IR2-B
- SCAGILE: Operational Security Tasks 4, 7
- SCFPSSD: Use Code Analysis Tools to Find Security Issues Early, Use Static Analysis Security Testing Tools, Perform Manual Verification of Security Features/Mitigations
- SCSIC: Peer Reviews and Security Testing & Vendor Software Delivery Integrity Controls

Question 3.10

- BSA: SC.1-3, SC.1-4, TV.3, TV.3-1, TV.5, SC.2, SC.4, SC.3, SC.3-2, EE.1, EE.1.2, EE.2, LO.1
- BSIMM10: AM1.3, AM1.5, AM2.1, AM2.2, AM2.5, AM2.6, AM2.7, AA1.2, AA2.1
- IDASOAR: Fact Sheet 1
- ISO 27034: 7.3.3, 7.3.5
- MSSDL: Practice 4 & 9
- NISTCSF: ID.RA-*
- NIST SP 800-53: SA-8, SA-15, SA-17
- NIST SP 800-160: 3.3.4, 3.4.5
- NIST SP 800-181: T0038, T0062, T0236, T0328; K0005, K0009, K0038, K0039, K0070, K0080, K0119, K0147, K0149, K0151, K0152, K0160, K0161, K0162, K0165, K0172, K0297, K0310, K0344, K0362, K0487, K0624; S0006, S0009, S0022, S0036,S0078, S0141, S0171, S0229, S0248; A0092, A0093, A107
- NIST SP-DEV-001; T0013, T0077, T0176; K0009, K0016, K0039, K0070, K0140, K0624; S0019, S0060, S0149, S0172, S0266; A0036, A0047
- OWASPASVS: 1.1.2, 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.11, 2 through 13
- OWASPTEST: Phase 2.4
- PCISSLRAP: 3.2
- SAMM15: DR1-A, DR1-B, TA1-A, TA1-B, TA3-B
- SCAGILE: Tasks Requiring the Help of Security Experts 3
- SCFPSSD: Threat Modeling, Establish Log Requirements and Audit Practices, Handle Data Safely, Handle Errors, Use Safe Functions Only
- SCTTM: Entire guide

Question 3.11

- BSA: SM.1, SM.2, SM.2-1, SM.2.4, SC.3-1, TV.2
- BSIMM10: CP2.4, SR2.5, SR3.2
- IDASOAR: Fact Sheets 19, 21
- NIST SP 800-53: SA-4, SA-12
- NIST SP 800-160: 3.1.1, 3.1.2, 3.3.8
- NIST SP 800-181: T0203, T0415; K0039; S0374; A0056, A0161; SP-DEV-002; K0153, K0266
- MSSDL: Practice 7
- OWASPASVS: 10, 14.2

- PCISSLRAP: 4.1
- SAMM15: SR3-A
- SCFPSSD: Manage Security Risk Inherent in the Use of Third-Party Components
- SCSIC: Vendor Sourcing Integrity Controls
- SCAGILE: Tasks Requiring the Help of Security Experts 8
- SCTPC: 3.2.2

Question 3.12

- BSA: SM.2, SM.2.1, SI.2, EN.1-1, LO.1
- BSIMM10: SFD1.1, SFD2.1
- IDASOAR: Fact Sheet 19
- MSSDL: Practice 5 & 6
- NIST SP 800-53: SA-12
- NIST SP 800-181: K0039, SP-DEV-001
- OWASPASVS: 10, 1.1.6
- SAMM15: SA1-A
- SCTPC: 3.2.1
- SCFPSSD: Establish Log Requirements and Audit Practices

Question 3.13

- BSA: TC.1-1, TC.1-3, TC.1-4, TC.1-5
- MSSDL: Practice 8
- NIST SP 800-181: K0039, K0070
- OWASPASVS: 1.14.3, 1.14.4, 14.1
- SCAGILE: Operational Security Task 3 & 8
- SCFPSSD: Use Current Compiler and Toolchain Versions and Secure Compiler Options
- SCSIC: Vendor Software Development Integrity Controls
- SCFPSSD: Use Current Compiler and Toolchain Versions and Secure Compiler Options

Question 3.14

- BSA: PD.1-5, TV.3, TV.5, TV.5-2, VM.1-3, VM.3
- BSIMM10: PT1.1, PT1.2, PT1.3, ST1.1, ST1.3, ST2.1, ST2.4, ST2.5, ST2.6, ST3.3, ST3.4
- IDASOAR: Fact Sheets 7, 8, 10, 11, 38, 39, 43, 44, 48, 55, 56, 57
- ISO 27034: 7.3.6
- NIST SP 800-53: SA-11, SA-15
- NIST SP 800-181: SP-DEV-001, SP-DEV-002; T0456; K0013, K0039, K0070, K0153, K0165, K0342, K0367, K0536, K0624; S0001, S0015, S0026, S0061, S0083, S0112, S0135, T0028, T0169,

T0176, T0253, T0266, T0516; K0009, K0039, K0272, K0339, K0342, K0362, K0536; S0046, S0051, S0078, S0081, S0083, S0135, S0137, S0167, S0242; A0015

- MSSDL: Practice 11
- PCISSLRAP: 4.1
- SAMM15: ST1-B, ST2-A, ST2-B
- SCAGILE: Operational Security Tasks 10, 11; Tasks Requiring the Help of Security Experts 4, 6, 7
- SCFPSSD: Perform Dynamic Analysis Security Testing, Fuzz Parsers, Network Vulnerability Scanning, Perform Automated Functional Testing of Security Features/Mitigations, Perform Penetration Testing
- SCSIC: Peer Reviews and Security Testing

Question 3.15

- BSA: CF.1, TC.1
- IDASOAR: Fact Sheet 23
- ISO 27034: 7.3.5
- OWASPTEST: Phase 4.2
- SCAGILE: Tasks Requiring the Help of Security Experts 12
- SCSIC: Vendor Software Delivery Integrity Controls, Vendor Software Development Integrity Controls
- NIST SP 800-181: SP-DEV-002; K0009, K0039, K0073, K0153, K0165, K0275, K0531; S0167, SP-DEV-001
- PCISSLRAP: 8.1, 8.2
- SCFPSSD: Verify Secure Configurations and Use of Platform Mitigation

Question 3.16

- BSA: VM.2, VM.2-1, VM.2-2, VM.1-1, VM.2-3, VM.2-4
- SCAGILE: Tasks Requiring the Help of Security Experts 10
- NIST SP 800-53: SA-10
- NIST SP 800-160: 3.3.8
- NIST SP 800-181: K0009, K0039, K0070, K0161, K0165; S0078
- PCISSLRAP: 4.1, 4.2
- SCAGILE: Operational Security Task 2
- SCFPSSD: Fix the Vulnerability, Identify Mitigating Factors or Workarounds
- SP800181: T0163, T0229, T0264; K0009, K0070

Question 3.17

- BSA: VM.2-1, PD.1-3
- BSIMM10: CMVM3.2
- MSSDLPG52: Phase Two: Design
- MSSDL: Practice 2

- NIST SP800181: T0047, K0009, K0039, K0070, K0343
- NIST SP800160: 3.3.8
- NIST SP800181: T0111, K0009, K0039, K0070, K0343, SP-DEV-001, SP-DEV- 002; K0009, K0039, K0070
- PCISSLRAP: 2.6, 4.2
- SAMM15: IM3-A
- SP800181: K0009, K0039, K0070

INFORMATION SECURITY

Question 4.1

- ISO 27001
- SOC 2 Type II
- CMMC Level 3-5, Cybersecurity Maturity Assessment

Question 4.2

- ISO IEC 27001, ISO 20243, ISO 27036
- NIST CSF1.1
- NIST 800-37, Rev. 2
- NIST SP 800-161
- SAE AS649, etc.

Question 4.3

- European Union General Data Protection Regulation (GDPR) regulation April 2016

Question 4.4

- NIST 800-53, NIST 800-171 DFARS, ISA/IEC 62443 or ISO 28001/2
- ISO 27003:2013 sec. 7.5.3, 8.2.2, 8.2.3, 8.3.1,14.1.2
- NIST SP 800-192: High-level requirements that specify how access is managed and who may access information under what circumstances.
- CNSSI 4009-2015 under multifactor authentication NIST SP 800-53 Rev. 4: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See authenticator.
- ISO 27003:2013 sect 9.2.1, 12.2.1, 13.1.1, Shared Assessments Standardized Control Assessment (SCA) sect. T.1
- Shared Assessments Standardized Control Assessment (SCA) sect. M.1
- NIST SP 800-12 Rev. 1 under Encryption ISO 7498-2: The cryptographic transformation of data to produce ciphertext.
- ISO 27003:2013 sect 10.1.2

Question 4.5

- CCMM:ID.AM
- ISA 99: 4.2.3.4 & SR 7.8, ISO 27001: A.8.1.1, A.8.1.2
- NIST CSF1.1
- NIST 800-53: CM8, CCS:2, BAI09.01, BAI09.02, BAI09.05

Question 4.6

- NIST 800-53 r5: RA-57

Question 4.7

- CCMM:ID.AM
- ISA 99: 4.2.3.4 & SR 7.8
- ISO 27001: A.8.1.1, A.8.1.2
- NIST CSF1.1
- NIST 800-53: CM8, CCS:2, BAI09.01, BAI09.02, BAI09.05

Question 4.8

- CCMM: ID.AM
- ISA 99: 4.2.3.4 & SR 7.8, ISO27001: A.8.1.1, A.8.1.2
- NIST CSF1.1, NIST 800-53: CM8, CCS:2, BAI09.01, BAI09.02, BAI09.05

Question 4.9

- NIST SP 800-60 r1

Question 4.10

- NIST 800-53 r5: SI 7(12)

Question 4.11

- NIST 800-53 r5:SI-5, PM – 16

Question 4.12

- CCMM: EDM1
- NIST 800-53:PL2, SA1
- CCMM: CPM3
- NIST 800-161 PE-16 Delivery and Removal,
- PE-17 Alternate Work Site,
- PE-18 Location of Information System Components)
- ISO 27001 A.11.1.6 - Delivery and loading areas
- A.11.2.3 - Cabling security
- A.11.2.8 - Unattended user equipment

Question 4.13

- NIST SP 800-53 r4: SI-12

Question 4.14

- NIST SP 800-128 under Vulnerability
- CNSSI 4009
- ISO 27003:2013 sect. 12.6.1
- Shared Assessments Standardized Control Assessment (SCA) sect. T.4

Question 4.15

- CNSSI 4009-2015
- ISO 27003:2013 sect 9.2.1, 12.2.1, 13.1.1, Shared Assessments Standardized Control Assessment (SCA) sect. T.1
- NIST SP 800-192
- NIST SP 800-53 Rev. 4: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See authenticator.
- Shared Assessments Standardized Control Assessment (SCA) sect. M.1

Question 4.16

- ISO 27003:2013 sect. 7.2.2

Question 4.17

- DFARS 252.246-7007

Question 4.18

- NIST SP 800-12 Rev. 1 under Encryption
- ISO 7498-2
- ISO 27003:2013 sect 10.1.2

Question 4.19

- NIST SP 800-152
- ISO 27003:2013 sect 9.1.2, 13.1.1
- ISO 27003:2013 sect13.1.3, Shared Assessments Standardized Control Assessment (SCA) sect. N.3
- NIST 800-53 or related controls
- NIST SP 800-152: A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.
- https://csrc.nist.gov/glossary/term/operational_technology

Question 4.20

- Shared Assessments Standardized Control Assessment (SCA) sect. V.2

Question 4.21

- ISO 27003:2013 sect 16.1.1

Question 4.22

- NIST SP 800-37 rev 2
- NIST SP 800-95: A method of testing where testers target individual binary components or the application, in whole, to determine whether intra or inter component vulnerabilities can be exploited to compromise the application, its data, or its environment resources.

Question 4.23

- Shared Assessments Standardized Control Assessment (SCA) sect. U.1

Question 4.24

- NIST CSF1.1

Question 4.25

- CNSSI 4009-2015 under incident handling
- NIST SP 800-61 Rev. 2.
- Shared Assessments Standardized Control Assessment (SCA) sect. K.4

Question 4.26

- Shared Assessments Standardized Control Assessment (SCA) sect. K.5

Question 4.27

- N/A

PHYSICAL SECURITY

Question 5.1

- DoD 5220.22-M, February 28, 2006 (National Industrial Security Program Operating Manual) Incorporating Change 2, May 18, 2016 (all applicable chapters, section, paragraphs).

Question 5.2

- NIST 800-53, rev. 4, PE-1, PE-2, PE-3.
- NIST Special Publication 800-53 Revision 3 PE-1, 2, 3
- American Petroleum Institute Pipeline SCADA Security Standard API 1164 2nd Edition 4, Annex A
- North American Electric Reliability Corporation (NERC) CIPS CIP 006-3c, A, B, R1
- NRC Cyber Security Programs for Nuclear Facilities Regulatory Guide 5.71 App. B.1.1, App. C.5.1
- ISO 27001 (specific clause desired here)
- NASA - CS-10 - Physical security measures - documented. Audited
- NASA - CS-11 - Physical access controls - documented and audited
- NASA- CS-15 - Background checks

Question 5.3

- ONSAT-PSP-14.3
- NIST 800-161 AT-3 - Security Training
- NASA -CS-4, incident response

Question 5.4

- Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) – CRR implementation guide: sect. 5 Incident Mgmt

Question 5.5 - Source of Question – ONSAT-PSP-14.5

- ONSAT-SDV-18.1
- NIST 800-161 (AC)

Questions 5.6, 5.7

- NIST 800-161 AC-3, PE-20
- NSIT 800-161 PE-3 Physical Access Control including tamper protection
- PE-20 Asset Monitoring and Tracking
- CM-8 Information System Component Inventory
- SA-18 Tamper Resistance and Detection
- SA-17 Developer Security Architecture
- SC-36 Distributed Processing and Storage)
- ISO 27001 - A.11.1.1 - Physical security perimeter
- A.11.1.1.2 - Physical Entry controls
- A.11.1.3 - Securing Offices, rooms and facilities·
- A.11.2.5 - Removal of assets
- NASA - CS-9 - Tamper resistant
- NASA - CS-10 - Physical Security measures in place
- NASA CS-11 - Access controls in place

Question 5.8

- NIST SP 800-53 (PV-2; SA-12(13))

Question 5.9

- NIST SP 800-53 (rev.4) (SA-12(1) Acquisition Strategies. Questions 1.13 - 1.19.1

Question 5.10

- IEC:IECEE, IECQ
- ISO 28000
- ISO 12931
- ISO 16678

PERSONNEL SECURITY

Questions 6.1 – 6.13

- BSA: PD.2-1, PD.2-2
- BSIMM10: CP3.2, SM1.1
- NISTCSF: ID.AM-6, ID.GV-2
- PCISSLRAP: 1.2
- SCSIC: Vendor Software Development Integrity Controls
- SP80053: SA-3
- SP800160: 3.2.1, 3.2.4, 3.3.1
- SP800181: K0233
- BSA: PD.2-2
- BSIMM10: CP2.5, SM1.3, T1.1, T1.5, T1.7, T2.6, T2.8, T3.2, T3.4
- MSSDL: Practice 1
- NISTCSF: PR.AT-*
- PCISSLRAP: 1.3
- SAMM15: EG1-A, EG2-A
- SCAGILE: Operational Security Tasks 14, 15; Tasks Requiring the Help of Security Experts 1
- SCFPSSD: Planning the Implementation and Deployment of Secure Development Practices
- SCSIC: Vendor Software Development Integrity Controls
- SP80053: SA-8
- SP800160: 3.2.4
- SP800181: OV-TEA-001, OV-TEA-002; T0030, T0073, T0320; K0204, K0208, K0220, K0226, K0243, K0245, K0252; S0100, S0101; A0004, A0057
- BSIMM10: SM1.2, SM1.3
- PCISSLRAP: 1.1
- SAMM15: SM1.A
- SP 800-181: T0001, T0004
- CDSE document on planning for Insider Threat program - https://www.cdse.edu/documents/cdse/sample-insider-threat-program-plan-for- industry.pdf
- NIST Cybersecurity Framework (2018) - https://www.nist.gov/cyberframework

SUPPLY CHAIN INTEGRITY

Question 7.1

- ISO 27036
- SAE AS6171

Question 7.2

- Microsoft's Trustworthy Computing Security Development Lifecycle, TSP for Secure Software Development

Question 7.3

- ONSAT - SDI 2.4

Question 7.4

- ONSAT - SDI 2.3

Question 7.5

- ISO 27036

Question 7.6

- NIST.SP.500-291r2 sect 6.5

Question 7.7

- ISO 27036, ONSAT – PSP 14.1

Question 7.8

- ISO 27036

Question 7.9

- ISO 27036
- ONSAT – AIA 4.1

Question 7.10

- ONSAT – AIA 4.1

Question 7.11

- R2:2013 - Sustainable Electronics Recycling International, sect 15

SUPPLY CHAIN RESILIENCE

Questions 8.1, 8.2

- Consistent with EO 13873 CISA Guidance (4/2020) and Supply Chain resilience
- Identify the people: 2. Manage the security and compliance: 3. Assess the components 4. Know the supply chain and suppliers. 5. Verify assurance of third parties. 6. Evaluate your SCRM program.

Questions 8.3, 8.4, 8.5

- NIST 800-161 (CP-8(4))
- NIST 800-161 (CP-8(3))

Questions 8.6, 8.7

- NIST 800-161 (PL-8(2))

- NIST 800-161 (PL-8(2)); Threat scenario 1 (Appendix B)

APPENDIX B: SUPPLEMENTAL INFORMATION (REASONING AND RATIONALE)

1. Qualifying Question

- **Question 1.1 –** These qualifying questions provide flexibility to respond to the survey by providing evidence of previous template submission or by providing evidence of qualifying SCRM industry or government certifications held by the responding organization.

2. Supply Chain Management and Supplier Governance

- **Question 2.1 –** This question is probing to ensure policies are regularly updated and communicated to customers to ensure regular maintenance of established processes/procedures for SCRM.
- **Questions 2.2, 2.3** - These questions ask whether the supplier has policies and procedures in place to address supply chain risks. If the company is fully compliant with ISO 9001, then we may have more confidence in their implementation, auditing, training, and change management processes. If the company is not fully compliant with ISO 9001, then we will have to dig deeper to understand whether they have effective implementation, audit plans, training, change management processes, etc. Supply chain risks can be introduced at any point in the SDLC. We need to ensure that the supplier is thinking about its supply chain throughout the lifecycle.
- **Question 2.4** - Ability to identify, track and validate that no components banned by the country of receipt reduces risk of receipt of vulnerable products/components, counterfeits and products or components that have been intentionally tampered with by bad actors.
- **Question 2.5** - These questions ask about the provenance of products and services to help manage supply chain risks, such as "unauthorized tampering and modification through the ICT supply chain, especially during repairs/refurbishing, updating," risks associated with lack of diversity, etc. Additionally, when invoking a SAAS capability, we recommend that the SBOM of the service is available to the user for local archive/logging for later analysis, in the event, that vulnerabilities are later identified.
- **Questions 2.6, 2.7** - These questions seek to understand aspects of BOM such as what attributes are in the BOM, what is being tracked, etc. We recognize that companies may need different categories in a BOM. For example, some companies may need "critical components" that may include customized components, components mounted with multiple other components, etc.
- **Questions 2.8, 2.9** - Stakeholders want to know that the supplier not only has a comprehensive and robust SCRM program for itself (which helps us to mitigate our own risk and meet customer expectations), but that it also requires the same from its sub-suppliers. We also want to ensure that the supplier ensures that "externally provided processes, products and services" conform to the SCRM requirements expected from the supplier and ensure that the supplier can meet the expectations of its customers. Suppliers must establish incident handling, including preparation, detection analysis, containment and recovery. We want incidents to be addressed with appropriate mitigations. Finally, we want to ensure that we are notified of changes in subcontractors because those changes could impact our ability to appropriately identify our own supply chain risks and our ability to meet the customers' expectations.

3. Secure Design and Engineering

- **Question 3.1 -** The ICT SCRM WG#4 System Design Writing Team identified questions that vendors might reasonably be asked to answer and/or elaborate upon with respect to their software and system design practices. The National Institute of Standards and Technology's

Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) white paper is the source for nineteen questions spanning four categories. The questions in this document are lifted nearly verbatim from the SSDF and arranged such that a lightweight Yes/No/Alt/NA response to each question would suffice for a simple inquiry. However, each question is also paired with a deeper question, which would be appropriate for a deeper inquiry and elicit a more elaborate response than a simple Yes, No, Alternate, or Not Applicable answer. Finally, the SSDF mappings to other documents and frameworks were also included as references to help vendors and evaluators. One question that was not taken from the SSDF is the "Level 0" question which (dis)qualifies the vendor from answering any questions in this section.

- **Question 3.2 –** N/A
- **Questions 3.3, 3.4** - Risk/Rationale: This includes requirements from internal sources (e.g., the organization's policies, business objectives, and risk management strategy) and external sources (e.g., applicable laws and regulations).
- **Question 3.5** - Risk/Rationale: Toolchains and tools may be used at different levels of the organization, such as organization-wide or project-specific.
- **Question 3.6** - Risk/Rationale: For code that is not intended to be publicly accessible, it helps prevent theft of the software and may make it more difficult or time-consuming for attackers to find vulnerabilities in the software.
- **Question 3.7** – N/A
- **Question 3.8** – N/A
- **Question 3.9** – N/A
- **Question 3.10** - Risk/Rationale: Addressing security requirements and risks during software design (secure by design) helps to make software development more efficient. These are particularly true for software that implements security functionality, such as cryptographic modules and protocols.
- **Question 3.11** – N/A
- **Question 3.12** – N/A
- **Question 3.13** – N/A
- **Question 3.14** - Risk/Rationale: Using automated methods lowers the effort and resources needed to detect vulnerabilities. Human-readable code includes source code and any other form of code an organization deems as humanly readable. Executable code includes binaries, directly executed bytecode, directly executed source code, and any other form of code an organization deems as executable.
- **Question 3.15** – N/A
- **Question 3.16** – N/A
- **Question 3.17** – N/A

4. Information Security

- **Question 4.1** – Risk/Rationale: there is no independent evaluation of holistic cybersecurity processes which meeting industry standards.
- **Question 4.2** – Risk/Rationale: Ad hoc or untested or incomplete/insufficient controls

- **Question 4.3** – Risk/Rationale: Lack of privacy controls can be assumptions of other types of missing information security controls. Companies at risk for EU GDPR violations, could suffer financial harm.
- **Question 4.4** – Risk/Rationale: Contaminated backups. Contamination of backup assets can slow recovery and prevent full restoration.
- **Question 4.5** – Risk/Rationale: Inadequate scope of procedures for managing enterprise network-connected assets.
- **Question 4.6** – Risk/Rationale: Non-IT professionals may bring in malware/viruses unintentionally from external downloads.
- **Question 4.7** – Risk/Rationale: Unable to identify rogue or at-risk equipment or inability to distribute patches in a timely manner.
- **Question 4.8** – Risk/Rationale: Unmanaged assets could be tampered with at any point in their lifecycle
- **Question 4.9** – Risk/Rationale: Lack of legal/regulatory compliance and potential security risk of using a product produced by a company on a banned list.
- **Question 4.10** – Risk/Rationale: Accidental or intentional introduction of vulnerabilities that could lead to failure or exploitation of mission critical functions
- **Question 4.11** – Risk/Rationale: No repeatable means of proactively identifying cybersecurity breaches. Lack of early detection of attacks, Lack of vetted detection techniques, etc.
- **Question 4.12** – Risk/Rationale Ensure physical security is coordinated with Information Security. May not apply to organizations that manage all valuable/critical cyber assets in a virtual environment. Reducing the risk of a cyber-attack on physical security systems and controls.
- **Question 4.13** – Risk: Breach of confidentiality ISO 27003:2013 sect 7.5.3
- **Question 4.14** – Risk/Rationale: Remote exploit or lateral exploit
- **Question 4.15** – Risk/Rationale: Unauthorized access. Nonstandard, non- comprehensive access control policies or procedures.
- **Question 4.16** – Risk/Rationale: Social Engineering, Carelessness, Adherence to Policy
    - **Question 4.16.1** – Risk/Rationale: If not refreshed, likely policies are not being consistently followed.
    - **Question 4.16.2** – Risk/Rationale: Improper/untrained access. Third-party workers accessing the same data as employees without proper training.
- **Question 4.17** – Risk/Rationale: Data Liability, Confidentiality
- **Question 4.18** – Risk/Rationale: Confidentiality of sensitive data
    - **Question 4.18.1** – Risk/Rationale –Some encryption keys can become a vulnerability source if not comprehensively managed.
    - **Question 4.18.2** – Risk/Rationale – Incomplete mitigation of risk if only data at rest or data in transit is protected.
- **Question 4.19** – Risk/Rationale: Remote exploit or lateral exploit.
- **Question 4.20** – Risk/Rationale: Presumed transfer of risk to cloud.
- **Question 4.21** - Risk/Rationale: Delay in, or inability to, recover.
- **Question 4.22** – Risk/Rationale: Undetected vulnerability.

- **Question 4.23** – Risk/Rationale: Patch management and detection of unauthorized software/releases (delta to inventory).
- **Question 4.25** – Risk/Rationale: Operational continuity during/after an attack.
- **Question 4.26** – Risk/Rationale: lack of ability to fully recover and validate system integrity. Loss of critical inputs from single or limited source suppliers (JIT Sensitivity).
- **Question 4.27** – Risk/Rationale: Customer could become liable for recovery costs.

5. Physical Security

Physical security is a mature activity however it has become more reliant on electronic and network connected systems. It is increasingly challenging to prevent overlapping of physical, cyber, and personnel security concerns as businesses become more reliant on Identity and Access Management (IDAM) systems to control facility access and report intrusion attempts. These systems which can update personnel status immediately and whose data flows across the organization's networks have demonstrated the need for these security "silos" to be more closely integrated.

Traditional physical security roles still exist, guards still have a role, but that role may require more understanding of how cyber-attacks work and behaviors associated with a trusted insider seeking to commit a malicious act. The ability of a guard to question, observe, and accurately report information may be highly relevant to a personnel or cyber security incident. Below is information about the reasoning behind the questions in the template.

- **Question 5.1** – Risk/Rationale: Green light questions that subsume most of the following questions (4.2-4.9).
- **Question 5.2** – Risk/Rationale: To ensure the company has policies and procedures that address the risk of how physical security responsibility includes and places a very high priority on preventing unauthorized access to cyber assets.
    - **Question 5.2.1** – Risk/Rationale: Not all policies and procedures are aligned with standards but if they are, this information is useful to understand the degree to which the policies may be effective.
- **Question 5.3** – Risk/Rationale: Ensure trustworthiness of individuals. Staff with non-cyber responsibilities may not be aware of the possible impact of seemingly inconsequential actions. Cybersecurity staff may not understand the full breadth of threats to the enterprise and how such threats may manifest as cyber impacts.
- **Question 5.4** – Risk/Rationale: Protection from a potential loss of revenue, reputation, and customer trust. Data protection is important both personally and professionally.
- **Question 5.5** – Risk/Rationale: A policy should direct responsibility and accountability. Those responsible and accountable should ensure that effective procedures to follow are established and promulgated to all staff. Cybersecurity staff may need to correlate physical security awareness with cybersecurity-related activity. Ensure the policy has been exercised to demonstrate its effectiveness in recovering from a potential incident.
- **Questions 5.6, 5.7** – Risk/Rationale: Ensure only authorized individuals have access to the facility, also ensure policies are documented. While a single mistake by an individual who harbors no malicious intent may warrant an informational sanction (i.e. warning) multiple breeches of security or other patterns may be important indicators of a significant risk. Having a formal policy and set of procedures reduces the likelihood that such a risk would go unnoticed?
- **Questions 5.8 – 5.10** These questions ask about the provenance of products and services to help manage supply chain risks, such as "unauthorized tampering and modification through the ICT

supply chain, especially during repairs/refurbishing, updating," risks associated with lack of diversity, etc. Additionally, when invoking a SAAS capability, we recommend that the SBOM of the service is available to the user for local archive/logging for later analysis, in the event, that vulnerabilities are later identified.

6. Personnel Security

- **Question 6.1** "General" questions intend to identify processes, policies, and documents on personnel as it relates to purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for information security. (NIST 800-53, Page F145).
- **Questions 6.2 - 6.5** "Onboarding" questions intend to measure how during the initial point of entry for new employees, they are introduced to the organization's security principles and culture.
    - **Question 6.6** "Offboarding" questions intend to illustrate the organization's preparedness with the potential risk(s) for terminated/discharged employees.
- **Questions 6.7- 6.13** "Awareness and Training" questions intend to meet the NIST CSF (2018) requirements and definition – the organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. (NIST CSF, 2018, Page 31)

7. Supply Chain Integrity

These questions check whether the supplier knows the companies in its own supply chain and has vetted those companies. This will help to mitigate supply chain risks such as diversity of our supply chain, geopolitical risks, etc. We also want to check whether the supplier vets the employees of their suppliers who might be provided as part of the service. This will help us to mitigate supply chain risks that stem from those employees (insider threats, etc.)

- **Question 7.1** – Risk/Rationale: Product visibility and traceability may not be comprehensive if not aligned to any frameworks or standards
- **Question 7.2** – Risk/Rationale: Lack of use of SDL could result in security vulnerabilities being missed somewhere within the lifecycle and inability to detect flaws early.
- **Question 7.3** – Risk/Rationale: Lack of documented validation processes creates an inability to detect product quality failures. Lack of proper disposition of non-conforming materials can result in release to customers.
- **Question 7.4** - Risk/Rationale: Lack of detection processes creates an inability to detect counterfeit product or product that has been tampered. Failure to notify customers could exacerbate impacts.
- **Question 7.5** – Risk/Rationale: Third-party HW/SW products may not have as stringent quality control and defect analysis and therefore could be at higher risk for non-conformance or being counterfeit.
- **Question 7.6** – Risk/Rationale: Cloud developed software poses additional potential integrity vulnerabilities due to possible data breach, account hijacking, poor credential management, and potential system vulnerabilities among other threats. Lack of proper controls on critical cloud infrastructures can result in unintended or unmanaged vulnerabilities for the end-product or service.

- **Question 7.7** - Risk/Rationale: Lack of regular and tracked training for all direct personal and relevant supplier personnel could lead to product integrity processes not being followed.
- **Question 7.8** – Risk/Rationale: Lack of evaluation of a supplier's product integrity could introduce undesired integrity vulnerabilities. Management reviews of supplier selection choices provide additional controls.
- **Question 7.9** – Risk/Rationale: Regular audits ensure that processes are being performed and running as desired and offer opportunities for improvements. Passing down audit requirements to suppliers ensures supplier integrity of your suppliers.
- **Question 7.10** – Risk/Rationale: On-going re-evaluation of integrity processes enables incorporation of changing standards, response to changing product requirements and a culture of continuous improvement.
- **Question 7.11** – Risk/Rationale: Lack of controlled disposal procedures could increase risks of counterfeiting and unintended uses.

8. Supply Chain Resilience

- **Questions 8.1 – 8.2** "Supply chain resilience" is defined as the ICT supply chain's ability to provide required ICT products and services under stress or failure (NIST 800-161, Page 3).The General questions are intended to measure the extent to which the company has a program in place to assess the architecture of its Critical ICT elements and assets.
- **Questions 8.3 – 8.5** "Business Continuity" questions are intended to address new concerns for organizations moving to remote or reduced work environments due to unplanned events. The questions are intended to ensure the presence of robust business continuity plans.

  Questions 8.6 – 8.7 The "supplier diversity" questions are intended to measure the processes companies use to limit the event of multiple suppliers being susceptible to the same threats (*e.g.,* geographic supplier diversity program.)