Cyber Supply Chain Survey Tool

User Guide

Cyber Risk Analytics and Measurement Program



**Table of Contents**

[1. Introduction 2](#_Toc160539068)

[1.1. Purpose and Scope 2](#_Toc160539069)

[1.2. Relation to Other NIST Publications 2](#_Toc160539070)

[1.3. Audience 2](#_Toc160539071)

[1.4. Document Organization 2](#_Toc160539072)

[1.5. Terminology 2](#_Toc160539073)

[2. Survey Tool Overview 2](#_Toc160539074)

[2.1. Changes from the UMD cyber supply chain assessment tool 3](#_Toc160539075)

[2.2. Anonymous entry 3](#_Toc160539076)

[2.3. Data Collection 3](#_Toc160539077)

[2.4. Secure data handling 4](#_Toc160539078)

[3. Application utilization 5](#_Toc160539079)

[3.1. Preparation 5](#_Toc160539080)

[3.2. Navigation instruction 5](#_Toc160539081)

[4. Further Research 8](#_Toc160539082)

[References 9](#_Toc160539083)

[Appendix A. List of Symbols, Abbreviations, and Acronyms 9](#_Toc160539084)

[Appendix B. Survey Questionnaire Mapping 9](#_Toc160539085)

List of Figures

[Fig. 1. Questionnaire Interaction 4](#_Toc149296420)

[Fig. 2. Cyber Supply Chain Survey Page 5](#_Toc149296422)

[Fig. 3. Sample Analysis](#_Toc149296424) 7

[Fig. 4. CPRT Sample 8](#_Toc149296425)

# Introduction

## Purpose and Scope

NIST is prototyping a survey tool and a knowledge resource to facilitate cybersecurity supply chain risk management. The tool provides insights for organizations to evaluate and manage their strategies and processes to minimize cybersecurity supply chain risks. It offers a series of questions for the participants to address in a trusted and anonymized environment and, based on the entered responses, provides the analysis and directs users to relevant guidance and standards for further research.

## Relation to Other NIST Publications

Cybersecurity Framework (CSF) 1.1 describes the five functions (identify, detect, protect, respond, recover) in which the survey questionnaires are grouped to provide more visibility into the organization’s practices in managing cybersecurity risks. CSF 2.0 has six functions with Govern added.

NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations guides organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain and serves as a reference in parsing the survey questionnaires to the organization risk management level’s activities.

## Audience

The survey tool is intended for federal organizations exploring processes to improve their supply chain risk management. Intended users of this tool are employees involved in supply chain management or organization risk management functions, including cyber practitioners who wish to analyze and assess cybersecurity risks in their organization’s supply chain.

## Document Organization

## Terminology

cybersecurity supply chain (CSSC); cybersecurity risk management (CSRM)

# Survey Tool Overview

The original version, the cyber supply chain assessment tool, was developed jointly with the University of Maryland College Park, R.H. Smith School of Business (UMD), as part of the research under NIST grant and GSA sponsorship [1]. The tool is composed of a survey questionnaire developed with the knowledge gained from decade-long research involving a process of regional field studies with industry over a several-year period and statistical analysis of the effect on an organization's breach profile based on the extent of its adoption of policies and practices as defined within the Cybersecurity Framework (CSF) [2].

The current iteration, the cyber supply chain survey tool, is cloud-based with a web interface for participants to enter the survey data anonymously and securely. The survey questions ask for information on a broad range of organization and cyber supply chain-related practices. The questions are grouped according to the NIST's five cybersecurity framework functions (Identify, Protect, Detect, Respond, Recover). The tool provides a score by categories within each CSF function from the participants' entered data.

## Changes from the UMD cyber supply chain assessment tool

The initial version of the organizational self-assessment tool was based on the Cybersecurity Framework (CSF) version 1.0. The latest questionnaire incorporates updates commensurate with CSF 1.1. Future updates will include considerations from CSF 2.0. To expand the use of the tool as a knowledge resource. A mapping tool is added as an additional capability to direct users to standards and sources for further research based on the survey analysis.

The original version was created using the Drupal 7 web content management system. The new version utilizes the latest version of Drupal 10, which has improved user experience and browser compatibility. The more recent version of Drupal also allows for underlying redesign to enhance security.

The additional security redesign includes improved isolation of the front-end user interface from the back end to minimize data leakage from the server. Further security hardening is implemented with encryption for data in transit and at rest.

Since no data was transferred from the original UMD tool, the benchmarking feature that compares respondents’ cyber security performance profiles against the entire sample of respondents and specific industries will not be made available in the initial phase.

## Anonymous entry

The application does not require users to log in or track their IP address or cookies to avoid collecting personally identifiable information (PII). Once the user session ends, all information that could be used to identify the user will become inaccessible and cannot be retrieved. This maximizes privacy and security for all users.

## Data Collection

The data collection function is in the form of a survey with a series of questions. The answers to the questions vary from simple yes/no, Likert scale selection to free text. This survey enforces input validation for format consistency.

## Secure data handling

This questionnaire use case describes the interactions of an anonymous user with the system as the participant utilizes the questionnaire survey interface to enter cyber incident information (Figure 1). The data is protected in a secure environment and is encrypted at rest and in transit. The token associated with the user session is randomly regenerated, so it cannot be retraced after the session closes.



Fig. 1. Questionnaire Interaction

# Application utilization

## Preparation

The survey questionnaire requires data from multiple departments and teams at different levels of the organization. Since the workflow is designed for a single-person entry for the organization, we highly recommend that the responses to the survey questionnaire are collected as part of preparation before data entry into the survey. The complete questionnaire can be viewed and downloaded from the survey website.

## Navigation instruction

The survey tool's web interface is compatible with Internet Explorer and Chrome. On the [Cyber supply chain survey](https://csrc.test-e1a.nist.gov/Projects/cybersecurity-risk-analytics/cyber-supply-chain-survey) tool page, click the “Expand all” button to see the entire survey. A PDF of the document can be downloaded by clicking the “Print this page” button on the survey questionnaire display page. See Figure 3.



Fig. 2. Cyber Supply Chain Survey Page

When all the information is collected and ready to be entered into the survey, proceed to the Cyber Supply Chain survey tool page and select “Start Cyber Supply Chain Survey.”

The survey tool is composed of six expandable sections. Five sections are from the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The additional section, the respondent profile, provides the metadata on the organization to add context to the assessment. To expand each section, click the left arrow associated with the section. The same process applies to the subsections. All questions must have a response, or a pop-up alert will appear, pointing the respondent to the incomplete section. See Figure 3.

Once the data is submitted, the tool will assess the alignment with the risk management processes and outcomes described in the NIST Cybersecurity Framework version 1.1. The five rings top display provides the scoring in each of the listed CSF categories from the individual responses to questions corresponding with each category and summed to an overall score. The values correlate to the level of adoption of the individual actions associated with each framework category. The displays are interactive and can be displayed as a complete report by clicking the “Show All” button or in parts by clicking on each category’s ring. This is shown in Figure 3.



Fig. 3. Sample Analysis

The survey result provides a view into the organization's breach profile based on the extent of its adoption of risk management policies described in the CSF. Insights to improve the risk profile can be found by clicking the "show details" button associated with each subcategory and following the hyperlinks to additional information on related guidance or standards sections. This is shown in Figure 4.

The printed report of the survey result (in PDF) retains the active hyperlinks for participants to conduct further research at a future date. Please note that the application removes the survey data upon browser closure, so printing should be done before closing the browser.



Fig. 4. CPRT Sample

# Further Research

The cyber supply chain survey tool leverages the Cybersecurity and Privacy Reference Tool (CPRT) to highlight the reference data from NIST publications. The added capability enables participants to interactively browse, search, and export the data in a structured format that is human- and machine-consumable. This tool combination allows users to draw upon multiple related NIST resources for further research to build or refine the cybersecurity management approach. Additional resources could be explored through the [National Online Informative Reference Program (OLIR)](https://csrc.nist.gov/projects/olir/), a NIST effort to facilitate subject matter experts (SMEs) in defining standardized online informative references between elements of their documents, products, and services and elements of NIST documents.

Appendix B provides the complete survey questionnaire grouped into the CSF 1.1 functions, categories, subcategories, and CSF 2.0 subcategories. For considerations into possible mitigations, mapping to the SP 800-53r5 controls is provided. Mapping to the SP 800-161r1 risk management levels offers additional insights into supply chain risk management practices improvements.

# References

1. University of Maryland College Park, R.H. Smith School of Business (2017). The Cyber Risk Predictive Analytics Project. Available at <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/UMD%20Final%20Report-Cyber%20Risk%20Analytics%20Project%20revised%20tc%20november%2025%202017.pdf>
2. Boyson S, Corsi TM, Paraskevas JP (2022). Defending digital supply chains: Evidence from a decade-long research program. *Technovation* 118. <https://doi.org/10.1016/j.technovation.2021.102380>
3. Colicchia C, Creazza A, Menachof DA (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal* 24 (2), 215–240. <https://doi.org/10.1108/SCM-09-2017-0289>
4. List of Symbols, Abbreviations, and Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CPRT Cybersecurity and Privacy Reference Tool

UMD University of Maryland College Park, R.H. Smith School of Business

CSF Cybersecurity Framework

1. Survey Questionnaire Mapping

Below is the mapping of the survey questionnaire to the CSF 1.1 functions, categories, subcategories, and CSF 2.0 subcategories. The mapping to SP 800-161r1 references the associated supply chain risk management levels, and the mapping to SP800-53r5 provides possible controls for further risk mitigation exploration. As with all mappings, these may not represent all possible mappings due to context and other factors.

|  |
| --- |
| **Respondent Profile** |
| How large is your organization?  |
| Are you a parent or subsidiary organization? |
| Are your networks/IT systems: |
| What is your organization's North American Industry Classification System (NAICS) Code? |
| What most accurately describes your job title / professional role? |
| Which business roles are the people from your organization who contributed to this questionnaire responsible for? Select all that apply. |
| Does your organization provide Software?  |
| Does your organization provide Hardware? |
| Does your organization provide Telecom/Data Network Provisioning? |
| Does your organization provide Other Services? |
| (If Yes) List other services |
| Does your organization currently supply IT products/services to the federal government? |
| Is your organization planning to supply IT products/services to the federal government? |
|   |
| **CSF Function** | **CSF Category** | **CSF v1.1 Sub Category** | **800-53r5 Control Identifier** | **Enterprise RM Level (800-161r1)** | **Questionnaire Numbering** | **Questionnaire** |
| I. Identify | A. Asset Management | ID.AM-1, ID.AM-2 | CM-8, PM-5 | 2,3 | IA1 | 1. Do you have an accounting or inventory of assets related to protected data? (Assets include network devices, servers, desktops, registers, operating systems, database software, and applications.)  |
|   |   | ID.AM- 5 | CP-2, RA-2, RA-9, SA-20, SC-6 | 1,2,3 | IA2 | 2. Does your asset management program identify and classify data, systems and processes according to risk/criticality? **If No or Not Applicable, skip to Question 3** |
|   |   | ID.AM-5 | CP-2, RA-2, RA-9, SA-20, SC-6 | 1,2,3 | IA2\_1 | 2.1 If yes, does this program specify security standards for each class of data? |
|   |   | ID.AM-5 | CP-2, RA-2, RA-9, SA-20, SC-6 | 1,2,3 | IA3 | 3. Do you have a process for regularly and frequently identifying vulnerabilities associated with assets related to protected data? |
|   |   | ID.AM-2 | CM-8 | 2,3 | IA4 | 4. Is software versioning and patching history recorded for all applicable IT assets? |
|   |   | ID.AM-2 | CM-8  | 2,3 | IA5 | 5. Do you know how many personal confidential records (PII, PHI or other similar) you hold in your systems?  |
|   |   | ID.AM-2 | CM-8  | 2,3 | IA6 | 6. Do you know the largest number of confidential records in any segregated database? |
|   |   | ID.AM-1, ID.AM-2, ID.AM-4 | CM-8, PM-5, AC-20, SA-9 | 2,3 | IA7 | 7. Do you use embedded digital signatures in hardware or software to uniquely identify and authenticate supply chain elements, processes, and actors? |
|   |   | ID.AM-5 | CP-2, RA-2, RA-9, SA-20, SC-6 | 1,2,3 | IA8 | 8. Do you have an Information Lifecycle Management plan that incorporates best practices for record retention, awareness and training, and database storage and destruction? |
|   |   | ID.AM-5 | CP-2, RA-2, RA-9, SA-20, SC-6 | 1,2,3 | IA9 | 9. Have you completed as Business Impact Analysis for all enterprise applications to prioritize business continuity actions? |
|   |   | ID.AM-3 | AC-4, CA-3, PL-8, SA-17 | 2,3 | IA10 | 10. Do you have an accurate, up-to-date network diagram? |
|   |   | ID.AM-3 | AC-4, CA-3, PL-8, SA-17 | 2,3 | IA11 | 11. Are all network/application communication flows documented and mapped? |
|   |   |   |   |   |   |   |
|   | B. Business Environment | ID.BE-1 | SR-1, SR-3 | 1,2,3 | IB1 | 1. Are your organization's business mission and objectives prioritized and communicated to stakeholders? |
|   |   | ID.BE-4 | CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2 | 1,2,3 | IB2 | 2. Have you identified supply chain dependencies for these organizational mission priorities? |
|   |   | ID.BE-4 | CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2 | 1,2,3 | IB3 | 3. Does your organization have a map with critical physical supply, distribution & service hubs/ nodes, and inter-related flows to help you visualize the IT supply chain? **If No or Not Applicable, skip to Question 4** |
|   |   | ID.BE-4 | CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2 | 1,2,3 | IB3\_1 | 3.1 If yes, how often is it updated? |
|   |   | ID.BE-5 | CP-2, CP-11, RA-9, SA-8, SA-20 | 1,2,3 | IB4 | 4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations? |
|   |   | ID.BE-5 | CP-2, CP-11, RA-9, SA-8, SA-20 | 1,2,3 | IB5 | 5. Do you have a supplier management program that:  |
|   |   |   |   | 1,2,3 | IB5\_1 | 5.1 Segments and prioritizes vendors of critical hardware/software/network services? |
|   |   |   |   | 1,2,3 | IB5\_2 | 5.2 Establishes and monitors external supplier cybersecurity standards? |
|   |   | ID.BE-1 | SR-1, SR-3 | 1,2,3 | IB6 | 6. How often does your organization use each of the following standards?  |
|   |   |   |   | 1,2,3 | IB6\_1 | 6.1 National Institute of Standards and Technology Cybersecurity Framework for Planning and Management |
|   |   |   |   | 1,2,3 | IB6\_2 | 6.2 IB4.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations |
|   |   |   |   | 1,2,3 | IB6\_3 | 6.3 IB4.3 ISO IEC 27001/27002 for 3rd Party Cybersecurity Management |
|   |   |   |   | 1,2,3 | IB6\_4 | 6.4 IB4.4 ISO 20244 Trusted Technology Provider Standard |
|   |   |   |   | 1,2,3 | IB6\_5 | 6.5 IB4.5 ISO/IEC 27036 Guidelines for Information Security and Supplier Relationships |
|   |   |   |   | 1,2,3 | IB6\_6 | 6.6 IB4.6 SAE AS649 Avoidance, Detection, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts |
|   |   |   |   | 1,2,3 | IB6\_7 | 6.7 Other Standard \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|   |   | ID.BE-1 | SR-1, SR-3 | 1,2,3 | IB7 | 7. Do you verify and validate the use of the standards from the previous question by any of the following means:  |
|   |   |   |   | 1,2,3 | IB7\_1 | 7.1 Self-Assessment? |
|   |   |   |   | 1,2,3 | IB7\_2 | 7.2 Self-Assessment with Third-Party Validation? |
|   |   |   |   | 1,2,3 | IB7\_3 | 7.3 Third-Party Assessment and Validation? |
|   | C. Governance | ID.GV-2 | PS-7, PS-9, PM-1, PM-2, PM-29 | 1,2 | IC1 | 1. Does your organization have a dedicated person who manages Information Security as their as a full time responsibility? **If No, skip to IC2** |
|   |   |   |   | 1,2 | IC1\_1 | 1.1 If yes, what is this person's estimated years of information security experience? Choices are: One to Three Years; Four to Nine; Ten to 19; 20 or more |
|   |   | ID.GV-1, ID.GV-2 | PS-7, PS-9, PM-2, PM-29, -1 controls from all security control families | 1,2,3 | IC2 | 2. Are c-suite/executive managers involved with the Information Security Officer in setting and communicating: |
|   |   |   |   | 1,2,3 | IC2\_1 | 2.1 IT security standards? |
|   |   |   |   | 1,2,3 | IC2\_2 | 2.2 Control structures? |
|   |   |   |   | 1,2,3 | IC2\_3 | 2.3 Roles and responsibilities? |
|   |   | ID.GV-2 | PS-7, PS-9, PM-1, PM-2, PM-29 |   | IC3 | 3. To what degree does the CIO/CSO organization coordinate actions with the following enterprise actors to manage cyber risk: Choices: Extensive Coordination to No Coordination on a Likert Scale 1 to 5 |
|   |   |   |   | 1,2,3 | IC3\_1 | 3.1 VP of Operations/Supply Chain |
|   |   |   |   | 1,2,3 | IC3\_2 | 3.2 Chief Risk Officer |
|   |   |   |   | 1,2,3 | IC3\_3 | 3.3 Chief Financial Officer |
|   |   |   |   | 1,2,3 | IC3\_4 | 3.4 Chief Executive Officer |
|   |   |   |   | 1,2,3 | IC3\_5 | 3.5 Chief Legal Officer |
|   |   |   |   | 1,2,3 | IC3\_6 | 3.6 Chief Compliance Officer |
|   |   |   |   | 1,2,3 | IC3\_7 | 3.7 Board Risk/Audit Committee |
|   |   | ID.GV-3 | -1 controls from all security control families | 1,2,3 | IC4 | 4. Are your organization's legal and regulatory requirements understood and used to prioritize cybersecurity risk management activities? |
|   |   |   |   |   |   | 4.1 To what extent are the legal and regulatory requirements used to prioritize cybersecurity risk management activities? (Likert scale: Always, Very Often, Sometimes, Rarely, Never) |
|   |   | ID.GV-1 | -1 controls from all security control families | 1,2,3 | IC5 | 5. Is an organizational information security policy documented? |
|   |   | ID.GV-4 | PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2 | 1,2,3 | IC6 | 6. Is the Board of Directors (BoD) (or equivalent governing body) regularly apprised of cyber risk conditions and defenses? |
|   |   | ID.GV-4 | PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2 | 1,2,3 | IC7 | 7. Do you have a cloud services controls matrix documenting: |
|   |   |   |   | 1,2,3 | IC7\_1 | 7.1 Inherited risk controls from your cloud service provider? |
|   |   |   |   | 1,2,3 | IC7\_2 | 7.2 Dual or joint risk controls? |
|   |   |   |   | 1,2,3 | IC7\_3 | 7.3 Board Risk/Audit Committee? |
|   | D. Risk Assessment | ID.RA-1 | CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | 1,2,3 | ID1 | 1. Is risk assessment a required component of your cyber system development life cycle (SDLC) plan? |
|   |   | ID.RA-2 | PM-15, PM-16, RA-10, SI-5 | 1,2,3 | ID2 | 2. Do you have a data-gathering mechanism to capture and consolidate information on risk events and exposures? |
|   |   | ID.RA-4 | CP-2, PM-9, PM-11, RA-2, RA-3, RA-9 | 1,2,3 | ID3 | 3. Do you have a formal methodology to evaluate risk information based on probability of occurrence and severity of risks to your cyber systems? |
|   |   | ID.RA-4 | CP-2, PM-9, PM-11, RA-2, RA-3, RA-9 | 1,2,3 | ID4 | 4. Are identified risks prioritized in order to inform risk management decisions? |
|   |   | ID.RA-1, ID.RA-3 | PM-12, PM-16, RA-3, RA-10, SI-5  | 1,2,3 | ID5 | 5. How often do you employ war gaming or other threat modeling exercises to identify the spectrum of potential attack vectors for your internal network and technology? Choices are Frequently to Never on Likert Scale 1 to 5 |
|   |   | ID.RA-4 | CP-2, PM-9, PM-11, RA-2, RA-3, RA-9 | 1,2,3 | ID6 | 6. Are you able to identify critical data that needs extra protection and more investment because of business and regulatory compliance, e.g. health profile data for HIPAA compliance?  |
|   |   | ID.RA-4 | CP-2, PM-9, PM-11, RA-2, RA-3, RA-9 | 1,2,3 | ID7 | 7. Can you calculate the direct/indirect value of your organization’s critical data e.g. the revenue it generates, the market share it contributes toward?  |
|   |   | ID.RA-5 | CA-2, CA-7, PM-16, PM-28, RA-2, RA-3 | 1,2,3 | ID8 | 8. Can you calculate the upper boundaries or maximum probable losses from critical IT system incidents or data breaches? |
|   |   | ID.RA-6 | CA-5, PM-4, PM-9, PM-28, RA-7 | 1,2,3 | ID9 | 9. Are your critical vendors identified and prioritized based upon:  |
|   |   |   |   | 1,2,3 | ID9\_1 | 9.1 Access to sensitive data? |
|   |   |   |   | 1,2,3 | ID9\_2 | 9.2 Criticality in maintaining continuity of the business?  |
|   |   |   |   | 1,2,3 | ID9\_3 | 9.3 Do you assess the cyber risks of your critical suppliers?  |
|   | E. Risk Management | ID.RM-1 | PM-9, PM-28 | 1 | IE1 | 1. Do you have a mission statement for your cyber security risk management program? |
|   |   | ID.RM-2 | PM-9 | 1 | IE2 | 2. Is the organization's risk tolerance identified and clearly documented? |
|   |   | ID.RM-1 | PM-9, PM-28 | 1 | IE3 | 3. Do you have a cyber risk management organizational chart with reporting relationships delineated? |
|   |   | ID.RM-3 | PM-8, PM-9, PM-11, RA-9 | 1,2,3 | IE4 | 4. Do you have a risk dashboard/registry? **If No Skip IF1** |
|   |   |   |   |   |   | Do your risk dashboard/registry do the following: |
|   |   |   |   | 1,2,3 | IE4\_1 | 4.1 Define key cyber risks? |
|   |   |   |   | 1,2,3 | IE4\_2 | 4.2 Identifiy responsible parties to manage the cyber risks? |
|   |   |   |   | 1,2,3 | IE4\_3 | 4.3 Show status of mitigation actions? |
|   | F. Supply Chain Risk Management | ID.SC-1 | PM-30, SA-9, SR-1, SR-2, SR-3, SR-5  | 1,2,3 | IF1 | 1. Do you have a process in place to identify, establish, assess, manage your trusted vendor as agreed to by organizational stakeholders? |
|   |   | ID.SC-2 | PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6 | 1,2,3 | IF2 | 2. Do you have a process to identify, prioritize, and assess suppliers and third-party partners of information systems and components using a cyber supply chain risk assessment process? |
|   |   | ID.SC-3 | SA-4, SA-9, SR-2, SR-3, SR-5 | 1,2,3 | IF3 | 3. As a acquirer/purchaser of vendor services, do you have contractually-mandated processes with suppliers and third-party partners to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan? |
|   |   | ID.SC-4 | AU-6, CA-2, CA-7, PS-7, SA-9, SA-11  | 1,2,3 | IF4 | 4. Do you routinely re-evaluate the management policies and performance of your suppliers to confirm that contractual obligations are met? |
|   |   | ID.SC-5 | CP-2, CP-4, IR-3, IR-4, IR-8, IR-9 | 1,2,3 | IF5 | 5. Do you conduct response and recovery planning and testing with your suppliers and third-party providers? |
|   |   |   |   |   |   |   |
| II. Protect |   |   |   |   |   |   |
|   | A. Identity Management, Authentication and Access Control | PR.AC-1 | IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12 | 1,2,3 | IIA1 | 1. Do you assign privileges and permissions based on user roles and credentials?  |
|   |   |   |   | 1,2,3 | IIA1\_1 | 1.1 If so, do you have an auditing process that supports revoking outdated identity and credentials? |
|   |   | PR.AC-7 | AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11 | 1,2,3 | IIA2 | 2. Do you incorporate single sign-on system for authenticating users across multiple accounts? |
|   |   | PR.AC-3 | AC-1, AC-17, AC-19, AC-20, SC-15 | 1,2,3 | IIA3 | 3. Is there a daisy chain, an interconnected set of written agreements among actors in your supply chain that assigns access control responsibilities and methods among all parties?  |
|   |   | PR.AC-5 | AC-4, AC-10, SC-7, SC-10, SC-20 | 2,3 | IIA4 | 4. Do you employ network access control (NAC) for remote connections? |
|   |   | PR.AC-3 | AC-1, AC-17, AC-19, AC-20, SC-15 | 1,2,3 | IIA5 | 5. Is the organization aware of all vendor remote access to internal devices, especially those that require a direct dial-in connection? |
|   |   | PR.AC-4 | AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 | 1,2,3 | IIA6 | 6. Are secure procedures in place to manage that vendor access (modem call-back for example)? |
|   |   | PR.AC-5 | AC-4, AC-10, SC-7, SC-10, SC-20 | 2,3 | IIA7 | 7. Are organizationally-defined traffic flows enforced, including that: |
|   |   |  |  | 2,3 | IIA7\_1 | 7.1 All traffic from the internet can only reach the internet-facing DMZ? |
|   |   |  |  | 2,3 | IIA7\_2 | 7.2 Traffic from systems on the DMZ cannot directly reach the internal network, but only through a middle-ware layer, etc.? |
|   |   | PR.AC-7 | AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11 | 1,2,3 | IIA8 | 8. Do you employ multifactor authentication: |
|   |   |   |   | 1,2,3 | IIA8\_1 | 8.1 For remote access to your network? |
|   |   |   |   | 1,2,3 | IIA8\_2 | 8.2 For internal users? |
|   |   |   |   | 1,2,3 | IIA8\_3 | 8.3 For vendors and third parties? |
|   |   |   |   | 1,2,3 | IIA8\_4 | 8.4 For super-users with privileged credentials? |
|   |   | PR.AC-5 | AC-4, AC-10, SC-7, SC-10, SC-20 | 2,3 | IIA9 | 9. Do you physically and logically segregate your sensitive network segments? |
|   |   | PR.AC-5  | AC-4, AC-10, SC-7, SC-10, SC-20 | 2,3 | IIA10 | 10. Is information of different sensitivity levels prohibited from residing on the same system? |
|   |   | PR.AC-1 | IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12 | 1,2,3 | IIA11 | 11. Do you establish remote site continuous auditing/surveillance methods: e.g., a code scanning engine at the supplier site to monitor work in progress? |
|   |   | PR.AC-2 | PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9 | 1,2,3 | IIA12 | 12. Do you have in place extra physical security controls (e.g., video surveillance of public areas; and location of servers in locked, inaccessible areas) over sensitive hardware/software/networks?  |
|   | B. Awareness and Training | PR.AT-1 | AT-2, PM-13, PM-14 | 1,2 | IIB1 | 1. Do you conduct training of receiving personnel in regard to detection of counterfeit or sub-grade hardware or software? |
|   |   | PR.AT-1 | AT-2, PM-13, PM-14 | 1,2 | IIB2 | 2. Do you conduct a Security Awareness program that is a requirement for all users of IT systems? |
|   |   | PR.AT-5 | AT-3, CP-3, IR-2, PM-13 | 1,2,3 | IIB3 | 3. Do you conduct a formal cybersecurity training program for those who have direct cyber operations responsibilities? |
|   |   | PR.AT-1 | PM-14 | 1,2 | IIB4 | 4. Are phishing tests a regular part of your awareness program? |
|   | C. Data Security | PR.DS-1 | MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28 | 1,2,3 | IIC1 | 1. Are data classified as critical/sensitive encrypted at rest? |
|   |   | PR.DS-2 |  SC-8, SC-11 | 2,3 | IIC2 | 2. Are data classified as critical/sensitive encrypted in transit? |
|   |   | PR.DS-1, PR.DS-2 | MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-8, SC11, SC-28 | 1,2,3 | IIC3 | 3. Do you encrypt software and software patches at rest and in motion throughout delivery?  |
|   |   | PR.DS-1, PR.DS-2 | MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-8, SC11, SC-28 | 1,2,3 | IIC4 | 4. In addition to data being protected at rest and in transit, are the encryption keys securely managed? |
|   |   | PR.DS-1, PR.DS-2 | MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-8, SC11, SC-28 | 1,2,3 | IIC5 | 5. Are the encryption keys stored separately from the data on a key-management server? |
|   |   | PR.DS-4 | CP-2, SC-5 | 2,3 | IIC6 | 6. Is encrypted data in transit carefully planned so as not to blind/hinder the organization's security technologies? |
|   |   | PR.DS-6 | SI-7 | 2,3 | IIC7 | 7. Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures? |
|   |   | PR.DS-5 | AC-4, AC-5, AC-6, AU-13, PS-6, SC-7, SI-4 | 1,2,3 | IIC8 | 8. Do you use anti-tamper mechanisms to counter data theft and subversion, including auto-destruction if tampering is detected? |
|   |   | PR.DS-2 |  SC-8, SC-11 | 2,3 | IIC9 | 9. Do you use tamper-resistant product packaging and digital seals to prevent or minimize in-transit intrusion? |
|   |   | PR.DS-5 | AC-4, AC-5, AC-6, AU-13, PS-6, SC-7, SI-4 | 1,2,3 | IIC10 | 10. Do you use Data Loss Prevention (DLP) software for data in use, in motion, and at rest? |
|   |   | PR.DS-5 | AC-4, AC-5, AC-6, AU-13, PS-6, SC-7, SI-4 | 1,2,3 | IIC11 | 11. Is egress traffic monitored (e.g., # of connections, length of connections, amount of traffic) to detect outbound connections that may be exfiltrating organizational data? |
|   |   | PR.DS-6 | SI-7, SI-10 | 2,3 | IIC12 | 12. Do you have documented baseline configuration standards for all devices connected to the corporate network? |
|   |   | PR.DS-6 | SI-7, SI-10 | 2,3 | IIC13 | 13. Do you follow OWASP (or similar) standards for coding of web applications? |
|   |   | PR.DS-5 | AC-4, AC-5, AC-6, AU-13, PS-6, SC-7, SI-4 | 1,2,3 | IIC14 | 14. Do you have network segmentation such that very critical data are located in subnets that are protected by their own firewall and intrusion detection system (IDS)? |
|   |   | PR.DS-5 | AC-4, AC-5, AC-6, AU-13, PS-6, SC-7, SI-4 | 1,2,3 | IIC15 | 15. Is sensitive data prohibited from residing on public-facing systems, such as the DMZ? |
|   |   | PR.DS-7 | CM-2 | 2,3 | IIC16 | 16. Is the production environment separate from other development and testing environments?  |
|   |   | PR.DS-7 | CM-2 | 2,3 | IIC17 | 17. Is production data only located in the production environment? |
|   |   | PR.DS-5 | AC-4, AC-5, AC-6, AU-13, PS-6, SC-7, SI-4 | 1,2,3 | IIC18 | 18. Do you turn off unnecessary functions in COTs or GOTs products to reduce or eliminate unauthorized access or exposure of the system? |
|   |   | PR.DS-6 | SI-7, SI-10 | 2,3 | IIC19 | 19. Are your network risk management controls automated? Likert 5-point scale. 5 always 3 sometimes 1 seldom |
|   |   | PR.DS-8 | SA-10 | 2,3 | IIC20 | 20. Do you have mechanisms or processes in place to check and verify that the hardware components of your purchased computing devices are genuine, function as intended, and have not been altered during the manufacturing and distribution processes? |
|   | D. Information Protection Processes | PR.IP-11 | PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21 | 1,2,3 | IID1 | 1. Do you conduct baseline security reviews (e.g. criminal, education, credit checks) of key IT personnel and high access users?  |
|   |   | PR.IP-11 | PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21 | 1,2,3 | IID2 | 2. How often do you update personnel security reviews? Likert Scale 5 = Continuously 3= Annually 1 = Never |
|   |   | PR.IP-3 | CM-3, CM-4, SA-10 | 2,3 | IID3 | 3. Do you use end to end Configuration Management (CM) systems to:  |
|   |   |   |   | 2,3 | IID3\_1 | 3.1 Track changes to software and settings? |
|   |   |   |   | 2,3 | IID3\_2 | 3.2 Record geo-spatial or IP address-based location information of actors? |
|   |   | PR.IP-3 | CM-3, CM-4, SA-10 | 2,3 | IID4 | 4. Are all proposed configuration changes required to be reviewed by a Change Control Board? |
|   |   | PR.IP-1 | CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 | 2,3 | IID5 | 5. Are technical solutions in place to enforce standard configurations? |
|   |   | PR.IP-7 | CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6 | 3 | IID6 | 6. Do you evaluate your suppliers' certifications in common IT standards (e.g. ISO/IEC 9001, ISO/IEC 27001, ISO 2800)?  |
|   |   | PR.IP-12 | RA-1, RA-3, RA-5, SI-2 | 1,2,3 | IID7 | 7. Do you evaluate measures of common vulnerabilities (CVSS scores) of your software suppliers? |
|   |   | PR.IP-12 | RA-1, RA-3, RA-5, SI-2 | 1,2,3 | IID8 | 8. Is a vulnerability management plan in place to feed risk management decisions? |
|   |   | PR.IP-10 | CP-4, IR-3, PM-14 | 2,3 | IID9 | 9. How often is cyber response/recovery planning and testing conducted with critical suppliers:  |
|   |   |   |   | 2,3 | IID9\_1 | 9.1 At contract initiation? |
|   |   |   |   | 2,3 | IID9\_2 | 9.2 During ongoing performance reviews? |
|   |   |   |   | 2,3 | IID9\_3 | 9.3 As needed? |
|   |   | PR.IP-4 |  CP-4, CP-6, CP-9 | 2,3 | IID10 | 10. Are regular backups of information conducted and tested? |
|   | E. Protective Technology | PR.PT-5 | CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6 | 2,3 | IIE1 | 1. Do you have backup or mirror sites to ensure continuity of operations in case of an incident at a primary site? |
|   |   | PR.PT-4 | AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47 | 2,3 | IIE2 | 2. Do you routinely encrypt sensitive communications **internally** using techniques such as DNSSEC, TLS, or SSL? |
|   |   | PR.PT-4 | AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47 | 2,3 | IIE3 | 3. Do you routinely encrypt sensitive communications with **vendors or customers** using techniques such as DNSSEC, TLS, or SSL?  |
|   |   |   |   | 2,3 | IIE4 | 4. Do you employ tools and techniques to determine if authentication tokens (e.g. passwords, biometrics) are sufficiently strong to resist attacks?  |
|   |   | PR.PT-3 | AC-3, CM-7 | 2,3 | IIE5 | 5. Do you quarantine non-conforming products until they can be verified through inspection/testing?  |
|   |   | PR.PT-4 | AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47 | 2,3 | IIE6 | 6. Do you quarantine code from outside suppliers in proxy servers to undergo virus scanning and authentication procedures? |
|   |   | PR.PT-2 | MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 | 2,3 | IIE7 | 7. Has an organizational policy for removable media been documented?  |
|   |   | PR.PT-2 | MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 | 2,3 | IIE8 | 8. Is the organizational policy for removable media enforced? |
|   |   | PR.PT-5 | CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6 | 2,3 | IIE9 | 9. Do you use standard components and parts across you IT product lines to increase resiliency of the supply chain? |
|   |   |   |   |   |   |   |
| III. Detect | A. Anomalies and Events | DE.AE-1 | AC-4, CA-3, CM-2, SC-16, SI-4 | 2,3 | IIIA1 | 1. Has an organizational baseline of expected data flows been established? |
|   |   | DE.AE-3 | AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4 | 1,2,3 | IIIA2 | 2. Do you use a Security Information and Event Management (SIEM) platform to aggregate and correlate security event information? If No, Skip the next Question |
|   |   |   |   | 1,2,3 |   | If yes, does your SIEM dashboard display event information:  |
|   |   |   |   | 1,2,3 | IIIA2\_1 | 2.1 For in-house units? |
|   |   |   |   | 1,2,3 | IIIA2\_2 | 2.2 For units managed by external service provider? |
|   |   | DE.AE-3 | AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4 | 1,2,3 | IIIA3 | 3. Do you receive current threat information from external industry/government/commercial sources? |
|   |   | DE.AE-3, DE.AE-5 | AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4 | 1,2,3 | IIIA4 | 4. Do you participate in Industry Specific Information Sharing and Analysis Centers (ISACs) for the purpose of sharing threat information? |
|   | B. Security and Continuous Monitoring | DE.CM-1 | AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 | 1,2,3 | IIIB1 | 1. Is a network-based IDS deployed, configured, and continuously monitored to detect security incidents? |
|   |   | DE.CM-4 | SC-44, SI-3, SI-4, SI-8 | 1,2,3 | IIIB2 | 2. Is anti-virus software deployed on endpoints to detect malicious code? |
|   |   | DE.CM-8 | RA-5 | 2,3 | IIIB3 | 3. How often do you use penetration testing on your operational systems to detect vulnerabilities? Likert scale 5 5 = always 3= Sometimes 1 = Never |
|   |   | DE.CM-7 | AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4 | 1,2,3 | IIIB4 | 4. Do you have testing/inspection processes for handling the receipt of electronic products, components, and spare parts that you purchase / acquire? |
|   |   | DE.CM-4, DE.CM-5, DE.CM-8 | SC-44, SI-3, SI-4, SI-8, RA-5, SC-18, SC-44, SI-3, SI-4 | 2,3 | IIIB5 | 5. Do you do in-house final inspection and conformity assessments of technology products & components that you manufacture prior to internal use or release to the customer? |
|   |   | DE.CM-4, DE.CM-8 | RA-5, SC-44, SI-3, SI-4, SI-8 | 2,3 | IIIB6 | 6. Do you use external evaluation labs (e.g., Common Criteria Certified Labs) to conduct conformity assessments of hardware and software prior to internal use or release to customer? |
|   |   | DE.CM-6 | CA-7, PS-7, SA-4, SA-9, SI-4 | 1,2,3 | IIIB7 | 7. Is acceptance testing of software built into contracts, with payments to suppliers withheld until test results are positive? |
|   |   | DE.CM-7 | AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4 | 1,2,3 | IIIB8 | 8. Do you extract and analyze all anomalies from audit logs, access reports, and security incident tracking reports? |
|   |   | DE.CM-5 | SC-18, SC-44, SI-4 | 1,2,3 | IIIB9 | 9. Do you screen mobile code and implement corrective actions to handle unacceptable code? |
|   | C. Detection Processes | DE.DP-2 | CA-1, CA-2, CA-7, PM-14, SI-1, SI-4, SR-1, SR-9, SR-10, all -1 controls | 1,2,3 | IIIC1 | 1. Is there a centralized corporate IT Incident Database that enables your organization to track the effectiveness of operational risk controls in place across your critical IT systems? |
|   |   | DE.DP-4 | AU-6, CA-2, CA-7, RA-5, SI-4 | 1,2,3 | IIIC2 | 2. Do your detection and information sharing processes extend to suppliers? |
|   |   | DE.DP-5 | CA-2, CA-7, PL-2, RA-5, SI-4, PM-14, CA-1 | 1,2,3 | IIIC3 | 3. Do you have Indicators of Compromise (IOCs) (e.g., virus signatures, IP addresses, URLs of botnet command servers, etc.) incorporated into the detection/monitoring process? |
|   |   |   |   |   |   |   |
| IV. Respond | A. Response Planning | RS.RP-1 | CP-2, CP-10, IR-4, IR-8  | 1,2,3 | IVA1 | 1. Do you have procedures for rating, reporting, and escalating events identified through detection/monitoring activities? |
|   |   | RS.RP-1 | CP-2, CP-10, IR-4, IR-8  | 1,2,3 | IVA2 | 2. Do you have a defined incident response team that has high level participation from all pertinent business functions and has clearly defined roles for response team members? |
|   |   | RS.RP-1 | CP-2, CP-10, IR-4, IR-8  | 1,2,3 | IVA3 | 3. Do you have an incident response plan that addresses system details and procedures for reporting and managing a suspected incident? |
|   | B. Communications | RS.CO-3 | CP-2, IR-4, IR-8 | 1,2,3 | IVB1 | 1. Do you have a crisis communications plan that can inform key internal/external stakeholders of the status of cyber breaches?  |
|   | C. Analysis | RS.AN-5 | CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 | 1,2,3 | IVC1 | 1. Do you require any counterfeit/grey market products that are detected and do not have forensic or evidentiary value be destroyed by reputable disposers? |
|   |   | RS.AN-5 | CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 | 1,2,3 | IVC2 | 2. Does your Corporate Audit/Risk Committee:  |
|   |   |   |   | 1,2,3 | IVC2.1 | 2.1 Examine the response to an incident? |
|   |   |   |   | 1,2,3 | IVC2.2 | 2.2 Identify residual risks? |
|   |   |   |   | 1,2,3 | IVC2.3 | 2.3 Implement additional controls to mitigate those residual risks? |
|   |   | RS.AN-5 | CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 | 1,2,3 | IVC3 | 3. Do you have a process to receive, analyze and respond to vulnerabilities disclosed by internal and external sources? |
|   |   |   |   |   |   |   |
|   | D. Mitigation | RS.MI-1,RS.MI-2 | IR-4 | 1,2,3 | IVD1 | 1. Do you have a corporate digital forensics capacity that performs the following:  |
|   |   |   |   | 1,2,3 | IVD1.1 | 1.1 Protocols for investigation and systems traceability/auditability |
|   |   |   |   | 1,2,3 | IVD1.2 | 1.2 Engagement of third-party law/accounting firms to determine value of claims? |
|   |   |   |   | 1,2,3 | IVD1.3 | 1.3 Notifications to third party insurer of loss of revenue? |
|   |   |   |   | 1,2,3 | IVD1.4 | 1.4 Notifications to Government Authorities (e.g., FBI) |
|   |   | RS.MI-1,RS.MI-2 | IR-4 | 1,2,3 | IVD2 | 2. Does your forensics capability rely on:  |
|   |   |   |   | 1,2,3 | IVD2.1 | 2.1 In-house security staff? |
|   |   |   |   | 1,2,3 | IVD2.2 | 2.2 Third party security organization with ongoing retainer? |
|   |   |   |   | 1,2,3 | IVD2.3 | 2.3 Forensic services contracted as needed? |
|   |   | RS.MI-1,RS.MI-2 | IR-4 | 1,2,3 | IVD3 | 3. Does your evidence handling process establish a "chain of custody" in your forensics management program? |
|   |   | RS.MI-2 | IR-4 | 1,2,3 | IVD4 | 4. Do you have processes in place for mitigating, disposing, and reporting fraudulent or counterfeit electronic hardware and software? |
|   | E. Improvements | RS.IM-1 | CP-2, IR-4, IR-8 | 1,2,3 | IVE1 | 1. Are major incident response performances debriefed with C-suite executives and the Board? |
|   |   | RS.IM-1 | CP-2, IR-4, IR-8 | 1,2,3 | IVE2 | 2. Do you have a lesson learned phase in which the incident response team reviews and modifies the incident response plan (IRP)? |
|   |   | RS.IM-2 | CP-2, IR-4, IR-8 | 1,2,3 | IVE3 | 3. If needed, are baseline configurations modified to prevent the same exploit or error? |
|   |   |   |   |   |   |   |
| V. Recover | A. Recovery Planning | RC.RP-1 | CP-10, IR-4, IR-8 | 1,2,3 | VA1 | 1. Do you update your IT system level disaster recovery plan at least annually? |
|   |   | RC.RP-1 | CP-10, IR-4, IR-8 | 1,2,3 | VA2 | 2. Do you have an IT system level data back-up/restore process that will allow for restoration of normal business processing in the event of disaster (including ransomware or DDoS)? |
|   | B. Improvements | RC.IM-1, RC.IM-2 | CP-2, IR-4, IR-8 | 1,2,3 | VB1 | 1. Are proposed solutions to breaches and cyber events tested to assure that the same exploit or error cannot happen again? |
|   | C. Communications | RC.CO-1 | IR-4 | 1,2,3 | VC1 | 1. Do you think your organization is positioned to file and settle cyber insurance claims faster than your competitors?  |
|   |   | RC.CO-3 | CP-2, IR-4  | 1,2,3 | VC2 | 2. Do you have cyber risk communications mechanisms in place to communicate recovery status with your employees and/or shareholders?  |
|   |   | RC.CO-3 | CP-2, IR-4  | 1,2,3 | VC3 | 3. Do you have cyber risk communications mechanisms in place to communicate recovery status with external partners and customers? |
|   |   |   |   |   |   |   |