National Institute of Standards and Technology
U.S. Department of Commerce

Feedback on Potential C-SCRM Risk Outcome Framework

Jon Boyens
Computer Security Division
IT Laboratory

SSCA Forum
24 January 2024

Initial Intent of a C-SCRM Risk Outcome Framework (ROF)

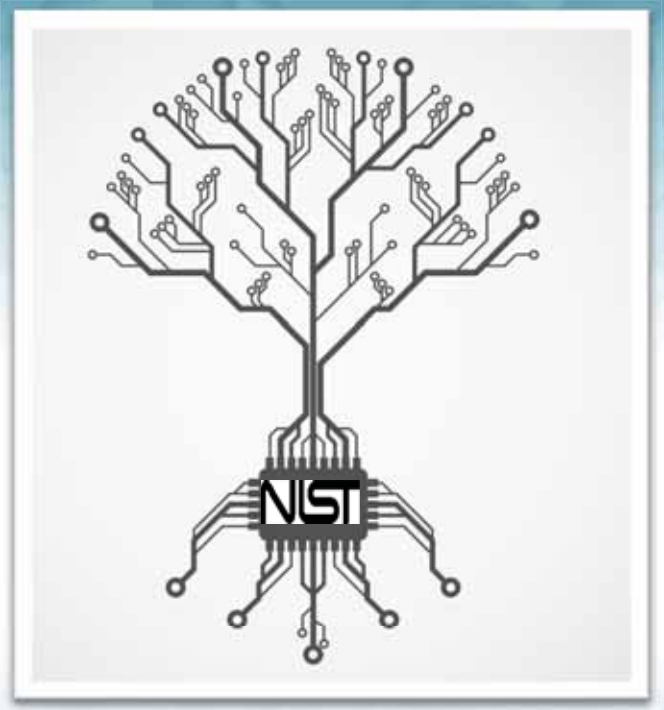
- Based on SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organization*
- CSCRM ROF: a framework for integrating C-SCRM risk with enterprise risk.
- A set of desired outcomes and applicable references that are common across all types of C-SCRM risk.
- Provide a common language for understanding, managing, and expressing CSCRM risk to internal and outside stakeholders.
- Used to help identify and prioritize actions for reducing C-SCRM risk
- A tool for aligning policy, business, and technological approaches to managing that risk.
- Help organizations address all forms of C-SCRM risk more effectively in their ERM.
- Improve the quality and consistency of C-SCRM risk information provided as inputs to ERM programs.

ROF Function and Category Unique Identifiers

Function	Category
GOVERN (GV)	Context (GV.CT)
	Roles and Responsibilities (GV.RR)
	Policy (GV.PO)
	Benchmarking (GV.BE)
	Communication (GV.CO)
	Adjustments (GV.AD)
	Oversight (GV.OV)
MANAGE (MA)	Risk Identification (MA.RI)
	Risk Analysis (MA.RA)
	Risk Prioritization (MA.RP)
	Risk Response (MA.RR)
	Risk Monitoring, Evaluation, and Adjustment (MA.RM)
	Risk Communication (MA.RC)
	Risk Improvement (MA.IM)

Concept Example: C-SCRM ROF

Function	Category	Subcategory	Implementation Example
MANAGE (MA): Continuously identify and address risks in accordance with the organization's risk management policies, processes, and priorities.	**Risk Identification (MA.RI):** Risk events for the organization are catalogued and recorded.	**MA.RI-1**: The assets (data, personnel, devices, systems, facilities, third-party services, etc.) that enable the organization to achieve its objectives are identified along with the assets' relative importance to those objectives and the organization's strategy.	The dependency between facility security and the electronic badge reader technology system is identified in a BIA, and any cyber risk to the electronic badge reader system is recorded in the Risk Description field of a risk register as something that could adversely affect building security.
		MA.RI-2: Threats against the organization's assets are identified and documented.	Threat intelligence sources are monitored for threats that may adversely affect critical assets. Threat modeling techniques are used to determine likely impact. This information is compared to information available from risk assessments and previous risk events. Relevant threat information is recorded in the Risk Description field of a risk register.
		MA.RI-3: Vulnerabilities of the organization's assets are identified and documented.	Vulnerability sources are monitored for vulnerabilities that affect critical assets, and relevant vulnerabilities are recorded in the Risk Description field of a risk register.
		MA.RI-4: Potential consequences are identified for each risk for the organization's assets and documented.	Risk cause and effect are documented as a risk scenario and included in the Risk Description field of a risk register.
		MA.RI-5: Risks are categorized in anticipation of future grouping and combination.	The Risk Category field of a risk register is populated with categories that are meaningful to an organization.
	Risk Analysis (MA.RA): Risk events are assessed for likelihood and impact.	**MA.RA-1**: The likelihood of each risk event is estimated using risk assessment techniques and probability models.	Bayesian models, event tree analysis, or similar techniques are used to determine the likelihood of a risk, and that information is recorded in the Current Assessment – Likelihood field in a risk register.



Email: scrm-nist@nist.gov

Visit: http://scrm.nist.gov