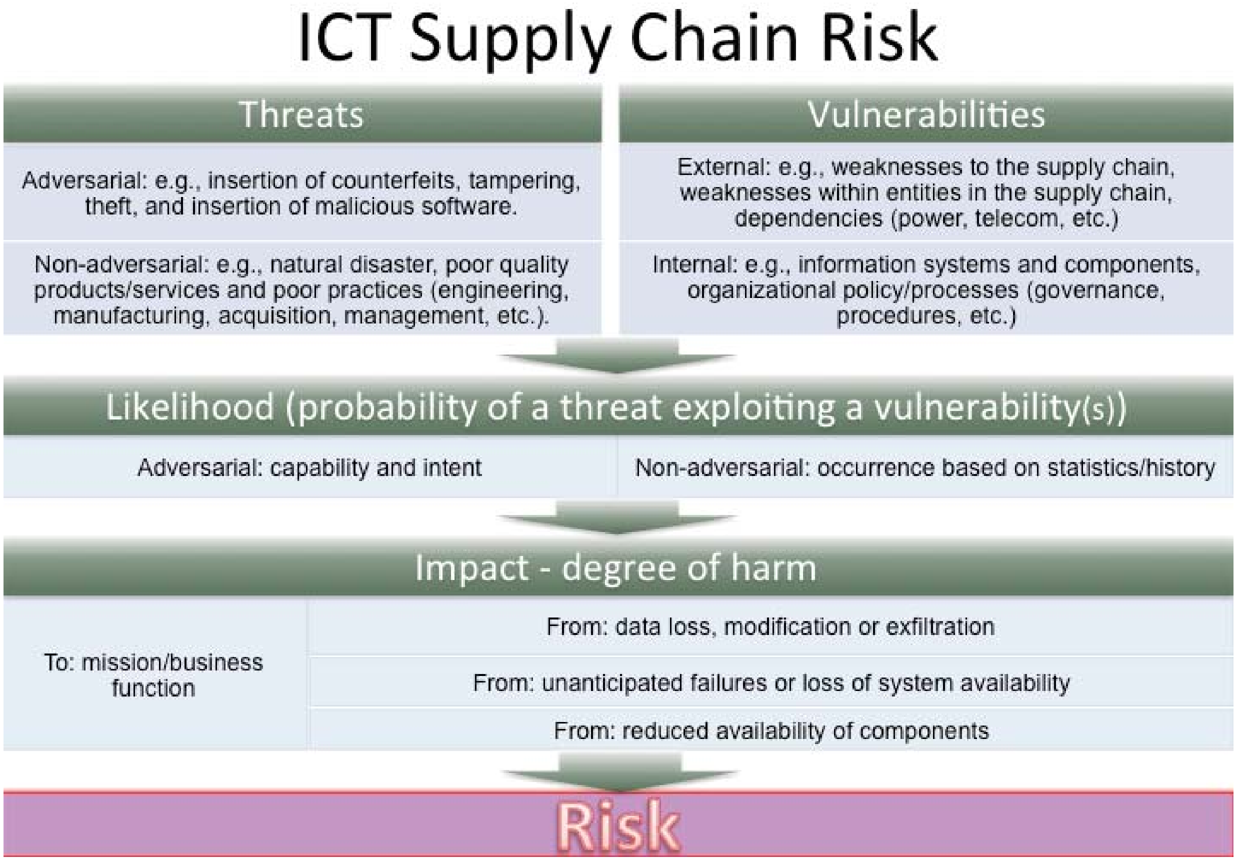
1.4.2 ICT Supply Chain Risk

ICT supply chain risks include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware (e.g., GPS tracking devices, computer chips, etc.), as well as poor manufacturing and development practices in the ICT supply chain. These risks are realized when threats in the ICT supply chain exploit existing vulnerabilities.

Figure 1-3 depicts ICT supply chain risk resulting from the likelihood that relevant threats may exploit applicable vulnerabilities and the consequential potential impact.



ICT Supply Chain Risk

Threats

Adversarial: e.g., insertion of counterfeits, tampering, theft, and insertion of malicious software.

Non-adversarial: e.g., natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc.).

Vulnerabilities

External: e.g., weaknesses to the supply chain, weaknesses within entities in the supply chain, dependencies (power, telecom, etc.)

Internal: e.g., information systems and components, organizational policy/processes (governance, procedures, etc.)

Likelihood (probability of a threat exploiting a vulnerability(s))

Adversarial: capability and intent

Non-adversarial: occurrence based on statistics/history

Impact - degree of harm

To: mission/business function

From: data loss, modification or exfiltration

From: unanticipated failures or loss of system availability

From: reduced availability of components

Risk

Figure 1-3: ICT Supply Chain Risk

It should be noted that it might take years for a vulnerability stemming from the ICT supply chain to be exploited or discovered. In addition, it may be difficult to determine whether an event was the direct result of a supply chain vulnerability. This may result in a persistent negative impact on an organization's missions that could range from reduction in service levels leading to customer dissatisfaction to theft of intellectual property or degradation of mission-critical functions.

CHAPTER TWO

INTEGRATION OF ICT SCRM INTO ORGANIZATION-WIDE RISK MANAGEMENT

ICT SCRM should be integrated into the organization-wide risk management process described in [NIST SP 800-39] and depicted in Figure 2-1. This process includes the following continuous and iterative steps:

(i) Frame risk – establish the context for risk-based decisions and the current state of the information system or ICT supply chain infrastructure;

(ii) Assess risk – review and interpret criticality, threat, vulnerability, likelihood, impact, and related information;

(iii) Respond to risk once determined – select, tailor, and implement mitigation controls; and

(iv) Monitor risk on an ongoing basis, including changes to an information system or ICT supply chain infrastructure, using effective organizational communications and a feedback loop for continuous improvement.

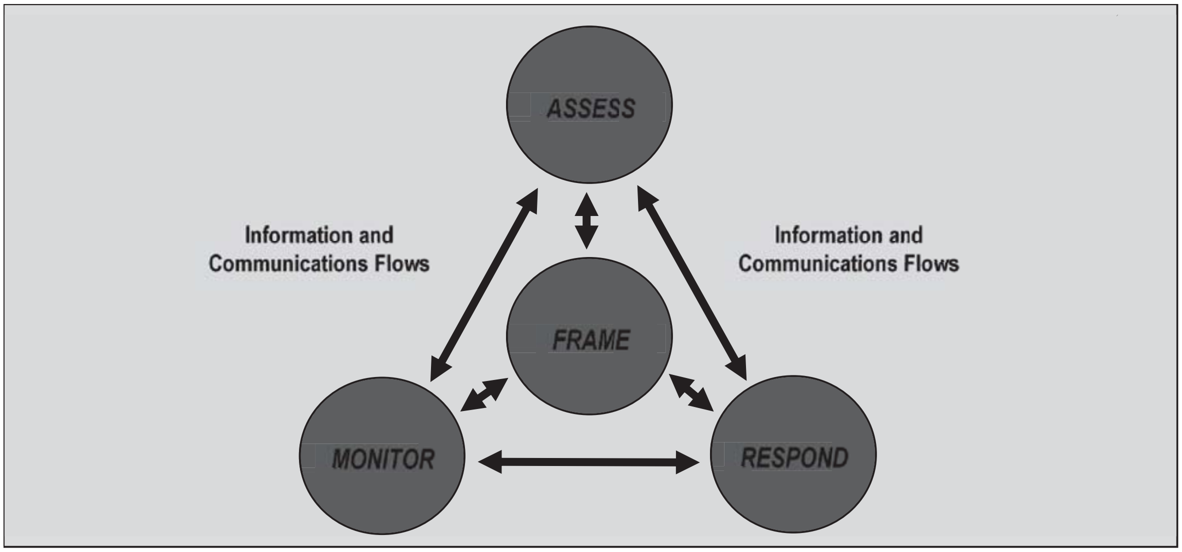

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Figure 2-1: Risk Management Process

Managing ICT supply chain risks is a complex, multifaceted undertaking that requires a coordinated effort across an organization and building trust relationships and communicating with external and internal partners and stakeholders. This includes: engaging multiple disciplines in identifying priorities and developing solutions; ensuring that ICT SCRM activities are performed throughout the SDLC; and incorporating ICT SCRM into overall risk management decisions. ICT SCRM activities should involve identifying and assessing applicable risks, determining appropriate mitigating actions, developing ICT SCRM Plans to document selected mitigating actions, and monitoring performance against ICT SCRM Plans. Because ICT supply chains differ across and within organizations, ICT SCRM plans should be tailored to individual organizational, program, and operational contexts. These tailored ICT SCRM Plans will provide the basis for determining whether an information system is "fit for purpose" [9] and as such, the controls need to be tailored accordingly. Tailored ICT SCRM plans will help organizations to focus appropriate resources on the most critical functions and components based on organizational mission/business requirements and their risk environment.

Organizations should ensure that tailored ICT SCRM Plans are designed to:

- Manage, rather than eliminate risk;
- Ensure that operations are able to adapt to constantly evolving threats;
- Be responsive to changes within their own organization, programs, and the supporting information systems; and
- Adjust to the rapidly evolving practices of the private sector's global ICT supply chain.

Chapter 2.1 describes the three-tier risk management approach in terms of ICT SCRM. Generally, senior leaders provide the strategic direction, mid-level leaders plan and manage projects, and individuals on the front lines develop, implement, and operate the ICT supply chain infrastructure. The activities performed in each tier can be integrated into an organization's overall risk management process in order to ensure that the ICT SCRM program appropriately supports the organization's mission and goals.[10] Chapter 2.2 describes the Risk Management Framework as it applies to ICT SCRM. The foundational concepts are described in greater detail in [NIST SP 800-39].

2.1 MULTITIERED RISK MANAGEMENT

To integrate risk management throughout an organization, [NIST SP 800-39] describes three organizational tiers, depicted in Figure 2-2, that address risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. ICT SCRM requires the involvement of all three tiers.

[9] The tailoring of ICT SCRM plans to individual organizational, program, and operational contexts may be referred to as "fit for purpose" as defined by Information Technology Infrastructure Library (ITIL) Service Strategy.[ITIL Service Strategy]

[10] This document uses the word "mission" to mean the organization's required tasks as determined by the organization's purpose and enterprise-level goals and priorities.

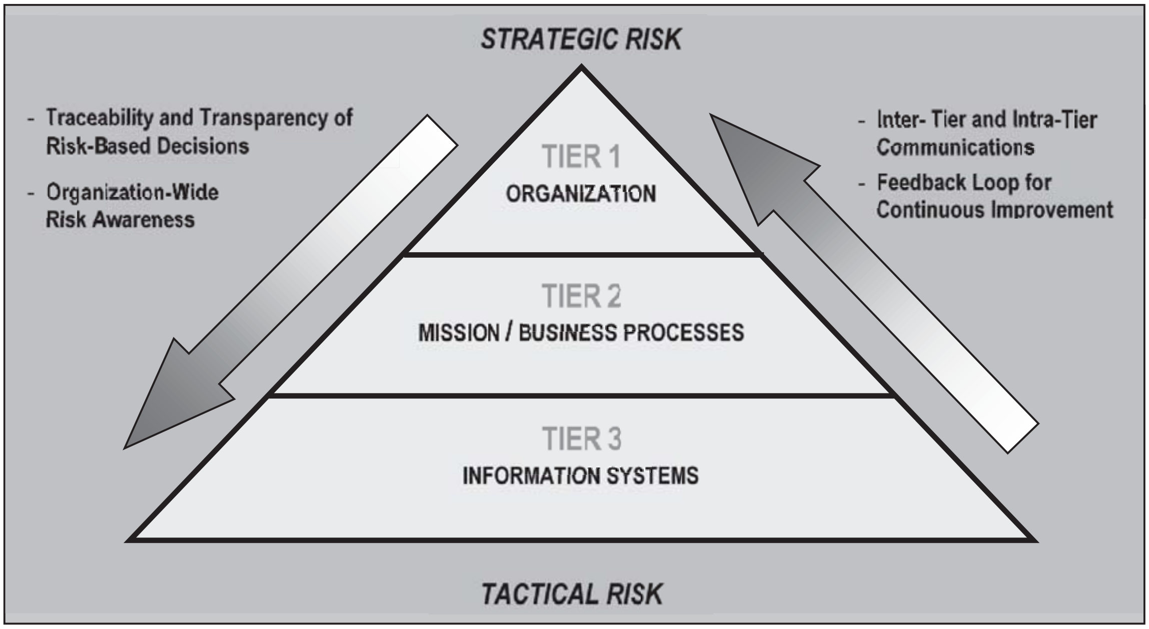

STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Figure 2-2: Multitiered Organization-wide Risk Management[11]

In general, Tier 1 is engaged in the development of the overall ICT SCRM strategy, determination of organization-level ICT SCRM risks, and setting of the organization-wide ICT SCRM policies to guide the organization’s activities in establishing and maintaining organization-wide ICT SCRM capability. Tier 2 is engaged in prioritizing the organization’s mission and business functions, conducting mission/business-level risk assessment, implementing Tier 1 strategy and guidance to establish an overarching organizational capability to manage ICT supply chain risks, and guiding organization-wide ICT acquisitions and their corresponding SDLCs. Tier 3 is involved in specific ICT SCRM activities to be applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems’ SDLCs.

The ICT SCRM activities can be performed by a variety of individuals or groups within an organization ranging from a single individual to committees, divisions, programs, or any other organizational structures. ICT SCRM activities will be distinct for different organizations depending on their organization’s structure, culture, mission, and many other factors. It should be noted that this publication gives organizations the flexibility to either develop stand-alone documentation (e.g., policies, assessment and authorization [A&A] plan and ICT SCRM Plan) for ICT SCRM, or to integrate it into existing agency documentation.

[11] Further information about the concepts depicted in Figure 2-2 can be found in [NIST SP 800-39].

Table 2-1 shows generic ICT SCRM stakeholders for each tier with the specific ICT SCRM activities performed within the corresponding tier. These activities are either direct ICT SCRM activities or have a direct impact on ICT SCRM.

Table 2-1: Supply Chain Risk Management Stakeholders

Tiers	Tier Name	Generic Stakeholder	Activities
1	Organization	Executive Leadership (CEO, CIO, COO, CFO, CISO, CTO, etc.) - Risk executive	Define corporate strategy, policy, goals and objectives
2	Mission	Business Management (includes program management [PM], research and development [R&D], Engineering [SDLC oversight], Acquisitions / Procurement, Cost Accounting, and other management related to reliability, safety, security, quality, etc.)	Develop actionable policies and procedures, guidance and constraints
3	Information Systems	Systems Management (architect, developers, system owner, QA/QC, test, and contracting personnel, approving selection, payment and approach for obtaining, maintenance engineering, disposal personnel, etc.)	Policy implementation, requirements, constraints, implementations

The ICT SCRM process should be carried out across the three risk management tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication, thus integrating both strategic and tactical activities among all stakeholders with a shared interest in the mission/business success of the organization. Whether addressing a component, a system, a process, a mission function, or a policy, it is important to engage the relevant ICT SCRM stakeholders at each tier to ensure that risk management activities are as informed as possible.

The next few sections provide example activities in each tier. However, because each organization is different, there may be activities that are performed in different tiers than listed as individual organizational context requires.

Chapter 3 provides a number of mission/business ICT SCRM controls that organizations can tailor for their use to help guide Tier 1, Tier 2, and Tier 3 ICT SCRM activities. It should be noted the tailoring should be scoped to the organization's risk management needs and take into consideration the costs associated with implementing ICT SCRM.

2.1.1 TIER 1 – ORGANIZATION

Tier 1 (Organization) provides strategic ICT SCRM direction for an organization using organizational-level mission/business requirements and policies, governance structures such as the risk executive (function), and organization-wide resource allocation for ICT SCRM. Tier 1 activities help to ensure that ICT SCRM mitigation strategies are cost-effective, efficient, and consistent with the strategic goals and objectives of the organization. It is critical that, as organizations define and implement organization-wide strategies, policies, and processes in this tier, they include ICT SCRM considerations.

ICT SCRM activities at this tier include:

- Establish ICT SCRM policies based on external and organizational requirements and constraints (e.g., applicable laws and regulations). Policies should include the purpose and applicability, as well as investment and funding requirements, of the ICT SCRM program;
- Based on the ICT SCRM policy, identify:
  - Mission/business requirements that will influence ICT SCRM, such as cost, schedule, performance, security, privacy, quality, and safety;
  - Information security requirements, including ICT SCRM-specific requirements; and
  - Organization-wide mission/business functions and how ICT SCRM will be integrated into their processes;
- Establish risk tolerance level for ICT supply chain risks;
- Establish a group of individuals across the organization who will address ICT SCRM throughout the organization, known as the ICT SCRM Team; and
- Ensure that ICT SCRM is appropriately integrated into the organization risk management policies and activities.

Implementing ICT SCRM requires that organizations establish a coordinated team-based approach to assess ICT supply chain risk and manage this risk by using programmatic and technical mitigation techniques. The coordinated team approach, either ad hoc or formal, will enable agencies to conduct a comprehensive analysis of their ICT supply chain, communicate with external partners/stakeholders, and gain broad consensus regarding appropriate resources for ICT SCRM.

The ICT SCRM Team should consist of members with diverse roles and responsibilities for leading and supporting ICT SCRM activities including information technology, information security, contracting, risk executive, mission/business, legal, supply chain and logistics, acquisition and procurement, and other relevant functions. These individuals may include government personnel or prime contractors hired to provide acquisition services to a government client.

Members of the ICT SCRM team should be a diverse group of people who are involved in the various aspects of the SDLC. Collectively, to aid in ICT SCRM, these individuals should have an awareness of, and provide expertise in organizational acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The ICT SCRM team may be an extension of an organization's existing information system risk management or include parts of a general risk management team.

2.1.2 TIER 2 – MISSION/BUSINESS PROCESS

Tier 2 (Mission/Business Process) addresses risk from a *mission/business process* perspective and is informed by the risk context, risk decisions, and risk activities at Tier 1.[12] In this tier, program requirements are defined and managed – including ICT SCRM as well as cost, schedule, performance, and a variety of critical nonfunctional requirements. These nonfunctional requirements include concepts such as reliability, dependability, safety, security, and quality. Many threats *to* and *through* the supply chain are addressed at this level in the management of trust relationships with system integrators,

[12] For more information, see [NIST SP 800-39 Section 2.2].

suppliers, and external service providers of ICT products and services. Because ICT SCRM can both directly and indirectly impact mission/business processes, understanding, integrating and coordinating ICT SCRM activities at this tier are critical for ensuring successful mission and business operations.

ICT SCRM activities at this tier include:

- Defining the risk response strategy, including ICT SCRM considerations, for critical processes;
- Establishing ICT SCRM processes to support mission/business processes;
- Determining the ICT SCRM requirements of the mission/business systems needed to execute the mission/business processes;
- Incorporating ICT SCRM requirements into the mission/business processes;
- Integrating ICT SCRM requirements into an enterprise architecture to facilitate the allocation of ICT SCRM controls to organizational information systems and the environments in which those systems operate; and
- Establishing a mission/business-specific ICT SCRM team that coordinates and collaborates with the organizational ICT SCRM team.

2.1.3 TIER 3 – INFORMATION SYSTEMS

Tier 3 (Information Systems) is where ICT SCRM activities are integrated into the SDLC of organizational information systems and system components. Many threats *through* the supply chain are addressed at this level with the use of ICT SCRM-related information security requirements. Risk management activities at Tier 3 reflect the organization's risk management strategy defined in Tier 1 (per NIST SP 800-39), as well as cost, schedule, and performance requirements for individual information systems as defined in Tier 2. ICT SCRM activities at this tier include:

- Applying, monitoring and managing ICT SCRM controls in the development and sustainment of systems supporting mission/business processes; and
- Applying, monitoring and managing ICT SCRM controls to the SDLC and the environment in which the SDLC is conducted (e.g., ICT supply chain infrastructure) used to develop and integrate mission/business systems.

At Tier 3, ICT SCRM significantly intersects with the SDLC, which includes acquisition (both custom and off-the-shelf), requirements, architectural design, development, delivery, installation, integration, maintenance, and disposal/retirement of information systems, including ICT products and services.

2.2 ICT SCRM ACTIVITIES IN RISK MANAGEMENT PROCESS

Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Figure 2-3 depicts interrelationships among the risk management process steps, including the order in which each analysis may be executed and the interactions required to ensure that the analysis is inclusive of the various inputs at the organization, mission, and operations levels.

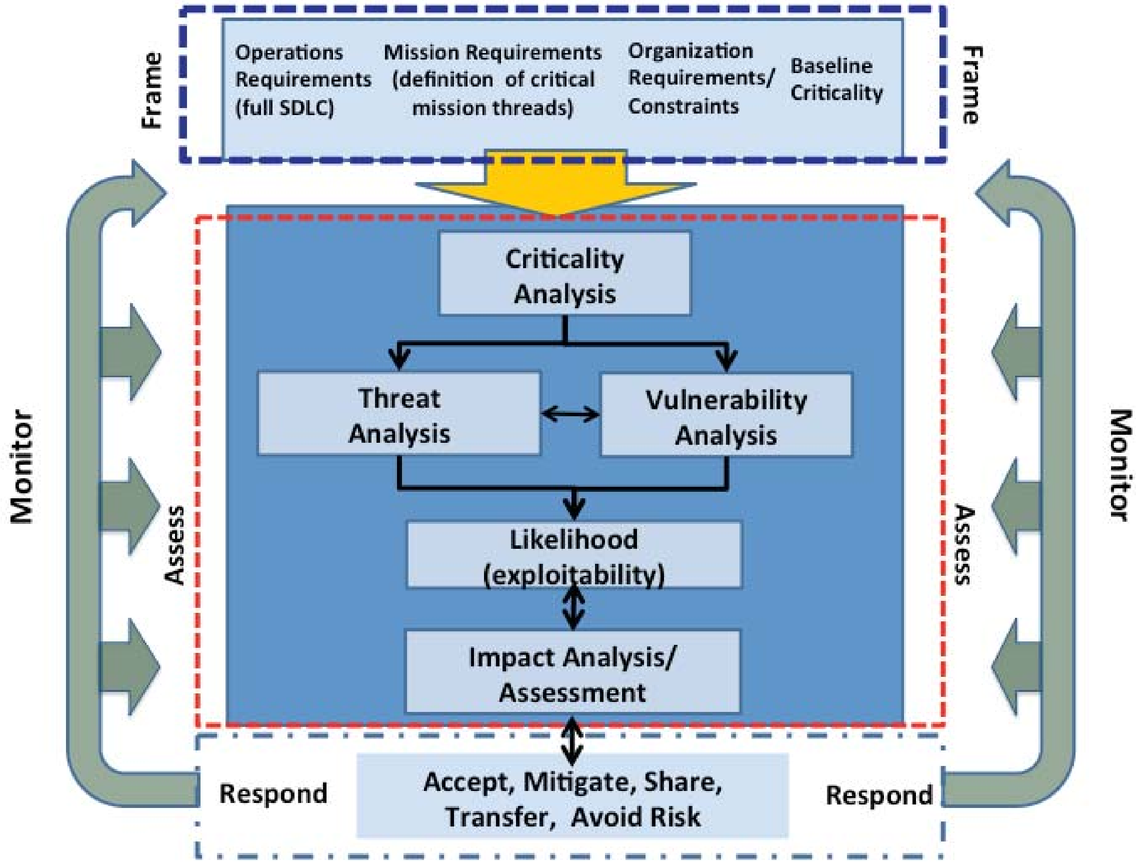
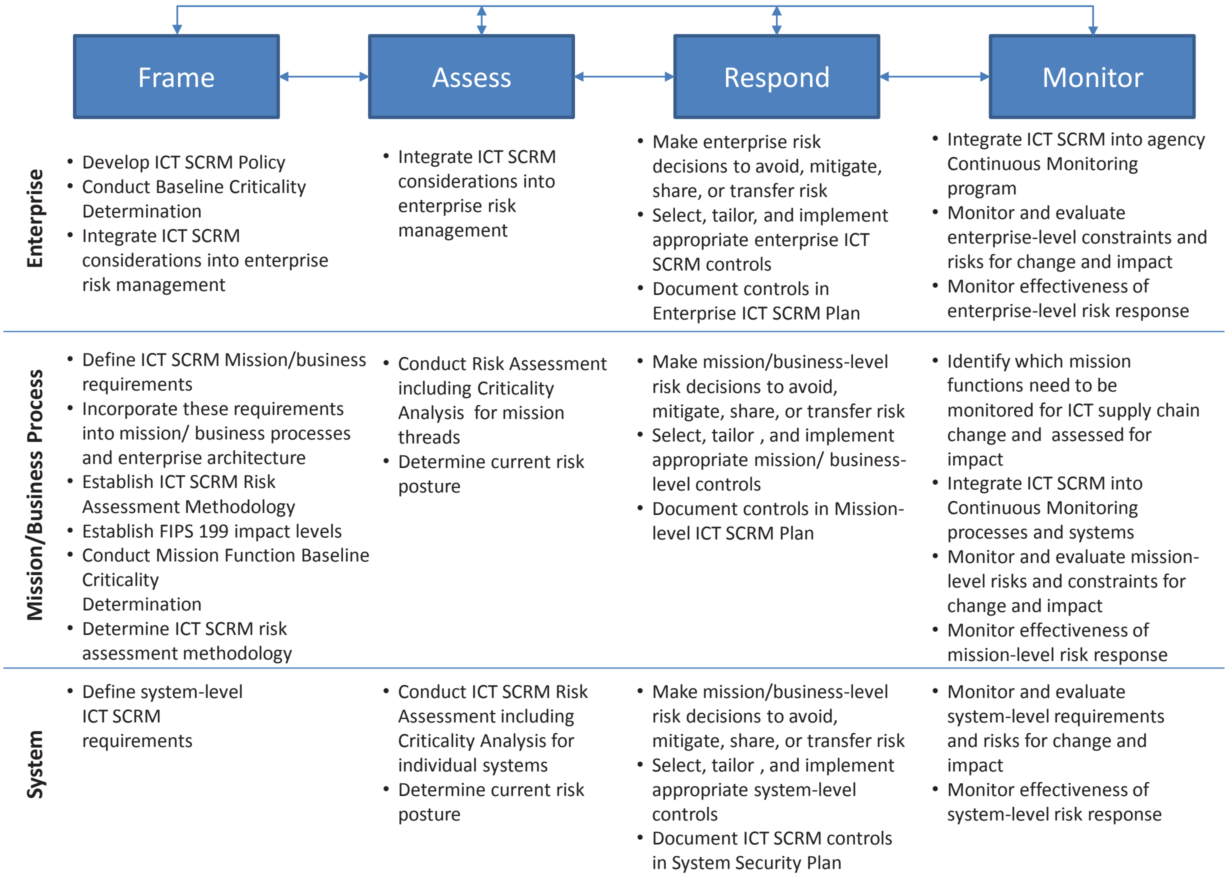

Frame
Operations Requirements (full SDLC)
Mission Requirements (definition of critical mission threads)
Organization Requirements/ Constraints
Baseline Criticality
Frame
Monitor
Assess
Criticality Analysis
Threat Analysis
Vulnerability Analysis
Likelihood (exploitability)
Impact Analysis/ Assessment
Assess
Monitor
Respond
Accept, Mitigate, Share, Transfer, Avoid Risk
Respond

Figure 2-3: ICT SCRM Risk Management

The steps in the risk management process – Frame, Assess, Respond, and Monitor - are iterative and not inherently sequential in nature. Different individuals may be required to perform the steps at the same time depending on a particular need or situation. Organizations have significant flexibility in how the risk management steps are performed (e.g., sequence, degree of rigor, formality, and thoroughness of application) and in how the results of each step are captured and shared—both internally and externally. The outputs from a particular risk management step will directly impact one or more of the other risk management steps in the risk management process.

Figure 2-4 summarizes ICT SCRM activities throughout the risk management process as they are performed within the three organizational tiers. The arrows between different steps of the risk management process depict simultaneous flow of information and guidance among the steps. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another. More details are provided in the following subsections.



	Frame	Assess	Respond	Monitor
Enterprise	• Develop ICT SCRM Policy • Conduct Baseline Criticality Determination • Integrate ICT SCRM considerations into enterprise risk management	• Integrate ICT SCRM considerations into enterprise risk management	• Make enterprise risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor, and implement appropriate enterprise ICT SCRM controls • Document controls in Enterprise ICT SCRM Plan	• Integrate ICT SCRM into agency Continuous Monitoring program • Monitor and evaluate enterprise-level constraints and risks for change and impact • Monitor effectiveness of enterprise-level risk response
Mission/Business Process	• Define ICT SCRM Mission/business requirements • Incorporate these requirements into mission/ business processes and enterprise architecture • Establish ICT SCRM Risk Assessment Methodology • Establish FIPS 199 impact levels • Conduct Mission Function Baseline Criticality Determination • Determine ICT SCRM risk assessment methodology	• Conduct Risk Assessment including Criticality Analysis for mission threads • Determine current risk posture	• Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor , and implement appropriate mission/ business-level controls • Document controls in Mission-level ICT SCRM Plan	• Identify which mission functions need to be monitored for ICT supply chain change and assessed for impact • Integrate ICT SCRM into Continuous Monitoring processes and systems • Monitor and evaluate mission-level risks and constraints for change and impact • Monitor effectiveness of mission-level risk response
System	• Define system-level ICT SCRM requirements	• Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems • Determine current risk posture	• Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor , and implement appropriate system-level controls • Document ICT SCRM controls in System Security Plan	• Monitor and evaluate system-level requirements and risks for change and impact • Monitor effectiveness of system-level risk response

Figure 2-4: ICT SCRM Activities in Risk Management Process

Figure 2-4 depicts interrelationships among the risk management process steps including the order in which each analysis is executed and the interactions required to ensure that the analysis is inclusive of the various inputs at the organization, mission, and operations levels.

The remainder of this section provides a detailed description of ICT SCRM activities within the Frame, Assess, Respond, and Monitor steps of the Risk Management Process. The structure of subsections 2.2.1 through 2.2.4 mirrors the structure of NIST SP 800-39, Chapters 3.1-3.4. For each step of the Risk Management Process (i.e., Frame, Assess, Respond, Monitor), the structure includes Inputs and Preconditions, Activities, and Outputs and Post-Conditions. Activities are further organized into Tasks according to [NIST SP 800-39] . NIST SP 800-161 cites the steps and tasks of the risk management process but rather than repeating any other content of [NIST SP 800-39], it provides ICT SCRM-specific guidance for each step with its Inputs and Preconditions, Activities with corresponding Tasks, and Outputs and Post-Conditions. NIST SP 800-161 adds one task to the tasks provided in [NIST SP 800-39], under the Assess step: Task 2-0, *Criticality Analysis*.

2.2.1 FRAME

Inputs and Preconditions

Frame is the step that establishes context for ICT SCRM in all three tiers. The scope and structure of the organizational ICT supply chain infrastructure, the overall risk management strategy, as well as specific program/project or individual information system needs, are defined in this step. The data and information collected during Frame provides inputs for scoping and fine-tuning ICT SCRM activities in other risk management process steps throughout the three tiers.

[NIST SP 800-39] defines risk framing as "the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk." ICT SCRM risk framing should be integrated into the overall organization risk framing process. Outputs of the organization's risk framing and the overall risk management process should serve as inputs into the ICT SCRM risk framing, including but not limited to:

- Organization policies, strategies, and governance;
- Applicable laws and regulations;
- Mission functions and business goals;
- Organization processes (security, quality, etc.);
- Organization threats, vulnerabilities, risks, and risk tolerance;
- Criticality of mission functions;
- Enterprise architecture;
- Mission-level security policies;
- Functional requirements; and
- Security requirements.

ICT SCRM risk framing is an iterative process that also uses inputs from the other steps of the risk management process (Assess, Respond, and Monitor) as inputs. Figure 2-5 depicts the Frame Step with its inputs and outputs along the three organizational tiers.

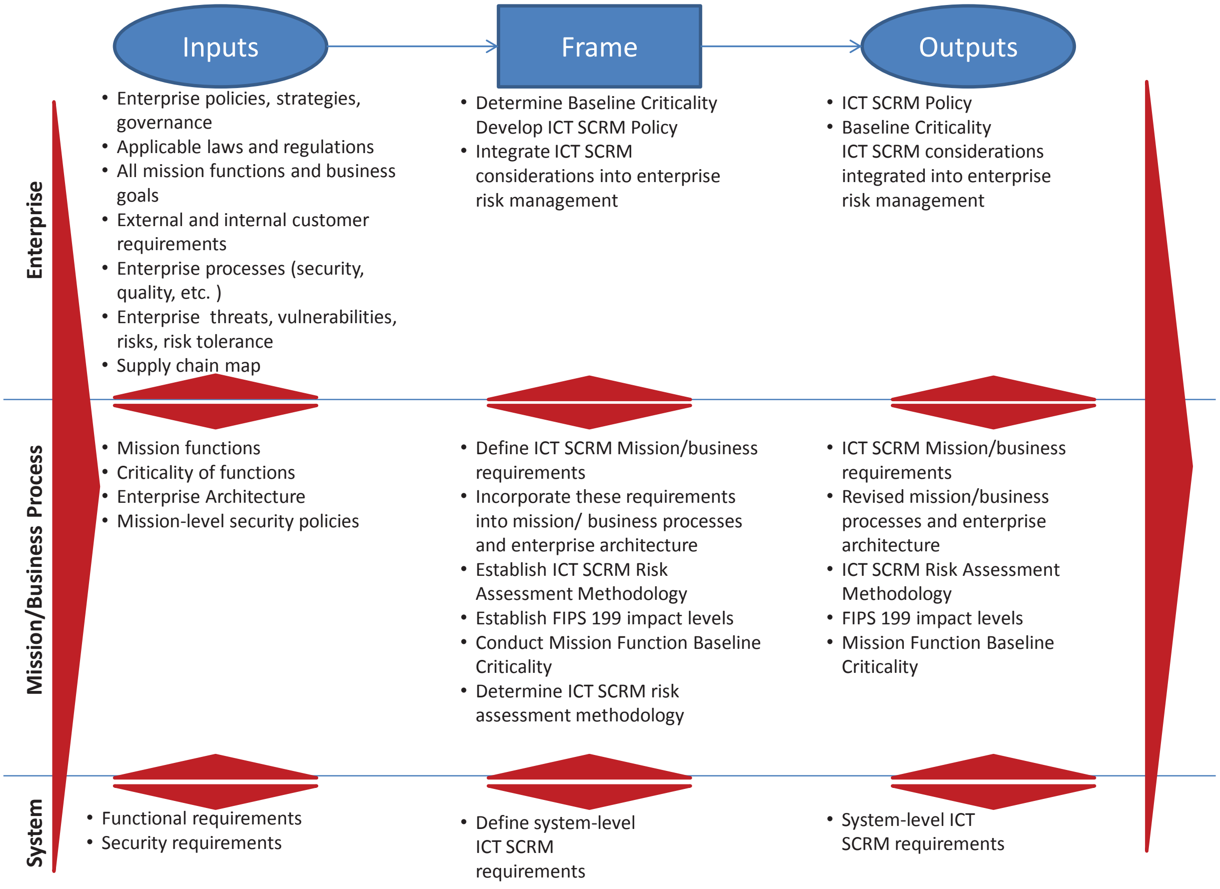

Inputs
Frame
Outputs
Enterprise
Mission/Business Process
System
• Enterprise policies, strategies, governance
• Applicable laws and regulations
• All mission functions and business goals
• External and internal customer requirements
• Enterprise processes (security, quality, etc.)
• Enterprise threats, vulnerabilities, risks, risk tolerance
• Supply chain map
• Determine Baseline Criticality Develop ICT SCRM Policy
• Integrate ICT SCRM considerations into enterprise risk management
• ICT SCRM Policy
• Baseline Criticality ICT SCRM considerations integrated into enterprise risk management
• Mission functions
• Criticality of functions
• Enterprise Architecture
• Mission-level security policies
• Define ICT SCRM Mission/business requirements
• Incorporate these requirements into mission/ business processes and enterprise architecture
• Establish ICT SCRM Risk Assessment Methodology
• Establish FIPS 199 impact levels
• Conduct Mission Function Baseline Criticality
• Determine ICT SCRM risk assessment methodology
• ICT SCRM Mission/business requirements
• Revised mission/business processes and enterprise architecture
• ICT SCRM Risk Assessment Methodology
• FIPS 199 impact levels
• Mission Function Baseline Criticality
• Functional requirements
• Security requirements
• Define system-level ICT SCRM requirements
• System-level ICT SCRM requirements

Figure 2-5: ICT SCRM in the Frame Step

Figure 2-5 depicts inputs, activities, and outputs of the Frame Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs and outputs to and from other steps of the Risk Management Process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Frame Step include inputs from other steps as well as inputs from the organization risk management process that are shaping the ICT SCRM process. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Activities

RISK ASSUMPTIONS

TASK 1-1: Identify assumptions that affect how risk is assessed, responded to, and monitored within the organization.

Supplemental Guidance:

As a part of identifying ICT supply chain Risk Assumptions within the broader Risk Management process (described in [NIST SP 800-39]), agencies should do the following:

- Define ICT SCRM mission, business, and system-level requirements;
- Identify which mission functions and related components are critical to the organization, including FIPS 199 impact level, to determine the **baseline criticality**;
- Identify, characterize, and provide representative examples of **threat sources**, **vulnerabilities**, **consequences/impacts**, and **likelihood** determinations related to ICT supply chain;
- Develop organization-wide ICT SCRM policy;
- Select appropriate ICT supply chain risk assessment methodologies, depending on organizational governance, culture, and diversity of the missions/business functions;
- Establish a method for the results of ICT SCRM activities to be integrated into the overall agency Risk Management Process; and
- Define which mission functions and information systems compose the ICT supply chain infrastructure, potentially including system integrator and external service provider support and periodically review its ICT supply chain infrastructure because it may evolve over time.

Baseline Criticality:

Critical functions are those functions, which if corrupted or disabled, are likely to result in mission degradation or failure. Mission-critical functions are dependent on their supporting systems that in turn depend on critical components in those systems (hardware, software, and firmware). Mission-critical functions also depend on processes that are used to execute the critical functions. Those components and processes that deliver defensive functions (e.g., access control, identity management, and crypto) and unmediated access (e.g., power supply) may also be considered mission-critical. A criticality analysis is the primary method by which mission-critical functions and associated systems/components are identified and prioritized.

Baseline criticality determination is the initial identification of specific critical components and processes based on the required function. This includes the analysis of requirements, architecture, and design to identify the minimum set of components required for system operation. Baseline criticality determination includes first identifying system requirements that support mission function and systems/components that have a direct impact on system requirements. This analysis should include agency system and ICT supply chain dependencies. Organizations should define the baseline criticality in the Frame phase to be updated and tailored to specific context in the Assess phase.

Determining baseline criticality is an iterative process performed at all tiers during both Frame and Assess. In Frame, baseline criticality determination is expected to be performed at a high level, using the available information with further detail incorporated through additional iterations or at the Assess step. Determining baseline criticality may include the following:

- Identify mission and business drivers, such as applicable regulations, policies, requirements, and operational constraints;
- Prioritize these drivers to help articulate the organization’s critical functions, systems, and components;
- Identify, group, and prioritize mission functions based on the drivers;
- Establish [FIPS 199] impact levels (high, moderate, low) for individual systems; and
- Map the mission functions to the system architecture and identify the systems/ components (hardware, software, and firmware) and processes that are critical to the mission/business effectiveness of the system or an interfacing network.

Please note that baseline criticality can be determined for existing systems or for future system integration efforts based on system architecture and design. It is an iterative activity that should be performed if a change warranting iteration is identified in the Monitor step.

Threat Sources:

For ICT SCRM, threat sources include: (i) hostile cyber/physical attacks either to the supply chain or to an information system component(s) traversing the supply chain; (ii) human errors; or (iii) geopolitical disruptions, economic upheavals, and natural or man-made disasters. [NIST SP 800-39] states that organizations provide a succinct characterization of the types of tactics, techniques, and procedures employed by adversaries that are to be addressed by safeguards and countermeasures (i.e., security controls) deployed at Tier 1 (organization level), at Tier 2 (mission/business process level), and at Tier 3 (information system level)—making explicit the types of threat sources that are to be addressed as well as making explicit those not being addressed by the safeguards/countermeasures.

Threat information includes historical threat data, factual threat data, or validated technology-specific threat information. Threat information may come from multiple information sources, including the U.S. Intelligence Community (for federal agencies), as well as open source reporting such as news and trade publications, partners, suppliers, and customers.

Information about ICT supply chain (such as from supply chain maps) provides the context for identifying possible locations or access points for threat agents to enter the ICT supply chain. The ICT supply chain threat agents are similar to the information security threat agents, such as attackers or industrial spies. Table 2-2 lists examples of ICT supply chain threat agents. Appendix D provides Supply Chain Threat Scenarios listed in Table 2-2.

Table 2-2: Examples of ICT Supply Chain Threat Agents

Threat Agent	Scenario	Examples
Counterfeiters	Counterfeits inserted into ICT supply chain (see Appendix D Scenario 1)	Criminal groups seek to acquire and sell counterfeit ICT components for monetary gain. Specifically, organized crime groups seek disposed units, purchase overstock items, and acquire blueprints to obtain ICT components that they can sell through various gray market resellers to acquirers.[13]
Insiders	Intellectual property loss	Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation.
Foreign Intelligence	Malicious code insertion (see	Foreign intelligence services seek to penetrate ICT supply chain and implant unwanted functionality (by inserting new

[13] "Defense Industrial Base Assessment: Counterfeit Electronics," [*Defense Industrial Base Assessment: Counterfeit Electronics*]

Threat Agent	Scenario	Examples
Services	Appendix D Scenario 3)	or modifying existing functionality) to be used when the system is operational to gather information or subvert[14] system or mission operations.
Terrorists	Unauthorized access	Terrorists seek to penetrate or disrupt the ICT supply chain and may implant unwanted functionality to obtain information or cause physical disablement and destruction through ICT.
Industrial Espionage/Cyber Criminals	Industrial Espionage/Intellectual Property Loss (see Appendix D Scenario 2)	Industrial spies/cyber criminals seek ways to penetrate ICT supply chain to gather information or subvert system or mission operations (e.g., exploitation of an HVAC contractor to steal credit card information).

Agencies can identify and refine ICT SCRM-specific threats in all three tiers. Table 2-3 provides examples of threat considerations and different methods that can be used to characterize ICT supply chain threats at different tiers.

Table 2-3: Supply Chain Threat Considerations

Tier	Threat Consideration	Methods
Tier 1	• Organization’s business and mission • Strategic supplier relationships • Geographical considerations related to the extent of the organization’s ICT supply chain	• Establish common starting points for identifying ICT supply chain threat. • Establish procedures for countering organization-wide threats such as insertion of counterfeits into critical systems and components.
Tier 2	• Mission functions • Geographic locations • Types of suppliers (COTS, external service providers, or custom, etc.) • Technologies used organization-wide	• Identify additional sources of threat information specific to organizational mission functions. • Identify potential threat sources based on the locations and suppliers identified through examining available agency ICT supply chain information (e.g., from supply chain map.) • Scope identified threat sources to the specific mission functions, using the agency the ICT supply chain information. • Establish mission-specific preparatory procedures for countering threat

[14] Examples of subverting operations include gaining unauthorized control to ICT supply chain or flooding it with unauthorized service requests to reduce or deny legitimate access to ICT supply chain.

Tier	Threat Consideration	Methods
		adversaries/natural disasters.
Tier 3	• SDLC	• Base the level of detail with which threats should be considered on the SDLC phase. • Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes.

Vulnerabilities

A *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [FIPS 200], [NIST SP 800-34 Rev. 1], [NIST SP 800-53 Rev 4], [NIST SP 800-53A Rev. 4], [NIST SP 800-115]. Within the ICT SCRM context, it is any weakness in the system/component design, development, manufacturing, production, shipping and receiving, delivery, operation, and component end-of life that can be exploited by a threat agent. This definition applies to both the systems/components being developed and integrated (i.e., within the SDLC) and to the ICT supply chain infrastructure, including any security mitigations and techniques, such as identity management or access control systems.

ICT supply chain vulnerabilities may be found in:

- The systems/components within the SDLC (i.e., being developed and integrated);
- The development and operational environment directly impacting the SDLC; and
- The logistics/delivery environment that transports ICT systems and components (logically or physically).

Organizations should identify approaches used to characterize ICT supply chain vulnerabilities, consistent with the characterization of threat sources and events and with the overall approach used by the organization for characterizing vulnerabilities. Appendix C provides examples of ICT supply chain threat events, based on [NIST SP 800-30 Rev. 1, Appendix B].

All three organizational tiers should contribute to determining the organization’s approaches to characterize vulnerabilities, with progressively more detail identified and documented in the lower tiers. Table 2-4 provides examples of considerations and different methods that could be used to characterize ICT supply chain vulnerabilities at different tiers.

Table 2-4: Supply Chain Vulnerability Considerations

Tier	Vulnerability Consideration	Methods
Tier 1	• Organization’s mission/business • Supplier relationships (e.g., system integrators, COTS, external services) • Geographical considerations related to the extent of the organization’s ICT supply chain • Enterprise/Security Architecture • Criticality Baseline	• Examine agency ICT supply chain information including that from supply chain maps to identify especially vulnerable locations or organizations. • Analyze agency mission for susceptibility to potential supply chain vulnerabilities. • Examine system integrator and supplier relationships for susceptibility to potential

Tier	Vulnerability Consideration	Methods
		supply chain vulnerabilities. • Review enterprise architecture and criticality baseline to identify areas of weakness requiring more robust ICT supply chain considerations.
Tier 2	• Mission functions • Geographic locations • Types of suppliers (COTS, custom, etc.) • Technologies used	• Refine analysis from Tier 1 based on specific mission functions and applicable threat and supply chain information. • Consider using the National Vulnerability Database (NVD), including Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS), to characterize, categorize, and score vulnerabilities[15]. • Consider using scoring guidance to prioritize vulnerabilities for remediation.
Tier 3	• Individual technologies, solutions, and suppliers should be considered.	• Use CVEs where available to characterize and categorize vulnerabilities. • Identify weaknesses.

Consequences and Impact

Impact is the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system [NIST SP 800-53 Rev.4].

For ICT SCRM, impact should be considered for the systems or components traversing the ICT supply chain, the supply chain itself, the ICT supply chain infrastructure, and the organization- or mission-level activities. All three tiers in the risk management hierarchy may be impacted. Potential impacts can be gathered through reviewing historical data for the agency, similar peer organizations, or applicable industry surveys. In this publication, impact is always in relation to the organization's mission and includes the systems or components traversing the supply chain as well as the supply chain itself.

The following are examples of ICT supply chain consequences and impact:

- An earthquake in Malaysia reduced the amount of commodity Dynamic Random Access Memory (DRAM) to 60 percent of the world's supply, creating a shortage for hardware maintenance and new design.
- Accidental procurement of a counterfeit part resulted in premature component failure, thereby impacting the organization's mission performance.

[15] See https://nvd.nist.gov/

Likelihood

In an information security risk analysis, likelihood is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability[CNSSI 4009]. Agencies should determine which approach(es) they will use to determine the likelihood of an ICT supply chain compromise, consistent with the overall approach used by the agency's risk management function.

RISK CONSTRAINTS

TASK 1-2: Identify constraints[16] on the conduct of risk assessment, risk response, and risk monitoring activities within the organization.

Supplemental Guidance:

Identify the following two types of constraints to ensure that the ICT supply chain is integrated into the agency risk management process:

1. Agency constraints; and
2. ICT supply chain-specific constraints.

Agency constraints serve as an overall input into framing the ICT supply chain policy at Tier 1, mission requirements at Tier 2, and system-specific requirements at Tier 3. Table 2-5 lists the specific agency and ICT supply chain constraints. ICT supply chain constraints, such as ICT SCRM policy and ICT SCRM requirements, may need to be developed if they do not exist.

Table 2-5: Supply Chain Constraints

Tier	Agency Constraints	ICT Supply Chain Constraints
Tier 1	• Organization policies, strategies, governance • Applicable laws and regulations • Mission functions • Organization processes (security, quality, etc.)	• Organization ICT SCRM policy based on the existing agency policies, strategies, and governance; applicable laws and regulations; mission functions; and organization processes.
Tier 2	• Mission functions • Criticality of functions • Enterprise architecture • Mission-level security policies	• ICT SCRM Mission/business requirements that are incorporated into mission/business processes and enterprise architecture.
Tier 3	• Functional requirements	• System-level ICT SCRM requirements.

[16] Refer to [NIST SP 800-39], Section 3.1, Task 1-2 for a description of constraints in the risk management context.

	• Security requirements	

An organization ICT SCRM policy is a critical vehicle for guiding ICT SCRM activities. Driven by applicable laws and regulations, this policy should support applicable organization policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission functions and business goals, along with the internal and external customer requirements. It should also define the integration points for ICT SCRM with the agency's Risk Management Process and SDLC.

ICT SCRM policy should define ICT SCRM-related roles and responsibilities of the agency ICT SCRM team, any dependencies among those roles, and the interaction among the roles. ICT SCRM-related roles will articulate responsibilities for collecting ICT supply chain threat intelligence, conducting risk assessments, identifying and implementing risk-based mitigations, and performing monitoring functions. Identifying and validating roles will help to specify the amount of effort that will be required to implement the ICT SCRM Plan. Examples of ICT SCRM-related roles include:

- Risk executive function that provides overarching ICT supply chain risk guidance to engineering decisions that specify and select ICT products as the system design is finalized;
- Procurement officer and maintenance engineering responsible for identifying and replacing the hardware when defective;
- Delivery organization and acceptance engineers who verify that the part is acceptable to receive into the acquiring organization;
- System integrator responsible for system maintenance and upgrades, whose staff resides in the acquirer facility and uses system integrator development infrastructure and the acquirer operational infrastructure;
- System Security Engineer/Systems Engineer responsible for ensuring that information system security concerns are properly identified and addressed; and
- The end user of ICT systems/components/services.

ICT SCRM requirements should be guided by the ICT SCRM policy, as well as by the mission functions and their criticality at Tier 2 and by known functional and security requirements at Tier 3.

RISK TOLERANCE

TASK 1-3: Identify the level of risk tolerance for the organization.

Supplemental Guidance:

Risk tolerance is the level of risk that organizations are willing to accept in pursuit of strategic goals and objectives [NIST SP 800-39]. Organizations should take into account ICT supply chain threats, vulnerabilities, constraints, and baseline criticality, when identifying the overall level of risk tolerance.[17]

[17] Federal Departments' and Agencies' governance structures vary widely (see [NIST SP 800-100, Section 2.2.2]). Regardless of the governance structure, individual agency risk decisions should apply to the agency and any subordinate organizations, but not in the reverse direction.

PRIORITIES AND TRADE-OFFS

TASK 1-4: Identify priorities and trade-offs considered by the organization in managing risk.

Supplemental Guidance

As a part of identifying priorities and trade-offs, organizations should consider ICT supply chain threats, vulnerabilities, constraints, and baseline criticality.

Outputs and Post Conditions

Within the scope of NIST SP 800-39, the output of the risk framing step is the *risk management strategy* that identifies how organizations intend to assess, respond to, and monitor risk over time. This strategy should clearly include any identified ICT SCRM considerations and should result in the establishment of ICT SCRM-specific processes throughout the agency. These processes should be documented in one of three ways:

1. Integrated into existing agency documentation;
2. A separate set of documents addressing ICT SCRM; or
3. A mix of separate and integrated documents, based on agency needs and operations.

The following information should be provided as an output of the risk framing step, regardless of how the outputs are documented:

- ICT SCRM Policy;
- Baseline Criticality including prioritized mission functions and FIPS 199 criticality;
- ICT supply chain risk assessment methodology and guidance;
- ICT supply chain risk response guidance;
- ICT supply chain risk monitoring guidance;
- ICT SCRM mission/business requirements;
- Revised mission/business processes and enterprise architecture with ICT SCRM considerations integrated; and
- System-level ICT SCRM requirements.

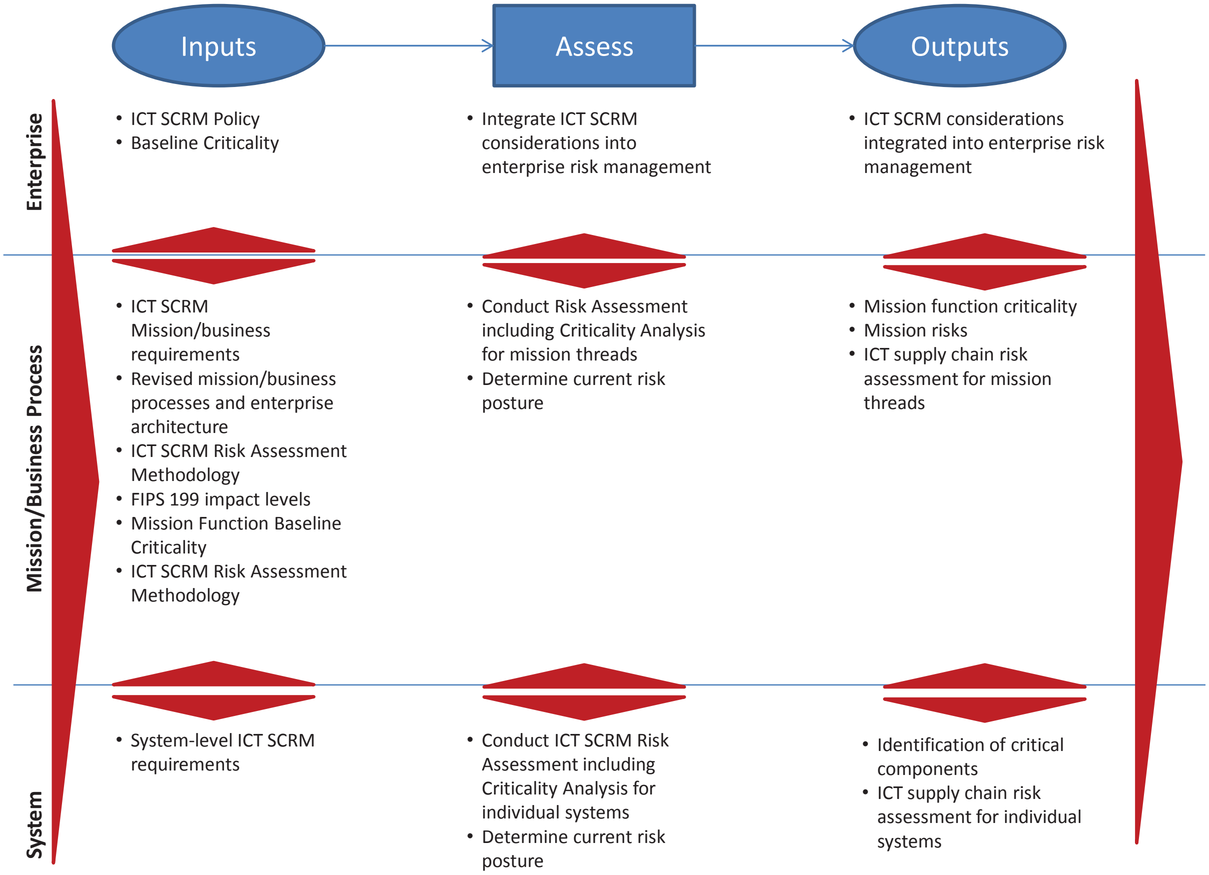
Outputs from the risk framing step serve as inputs to the risk assessment, risk response, and risk monitoring steps.

2.2.2 ASSESS

Inputs and Preconditions

Assess is the step where all the collected data is used to conduct a risk assessment. A number of inputs are combined and analyzed to identify the likelihood and the impact of an ICT supply chain compromise, including criticality, threat, and vulnerability analysis results; stakeholder knowledge; and policy, constraints, and requirements.

An ICT supply chain risk assessment should be integrated into the overall organization risk assessment processes. ICT SCRM risk assessment results should be used and aggregated as appropriate to communicate ICT supply chain risks at each tier of the organizational. Figure 2-6 depicts the Assess Step with its inputs and outputs along the three organizational tiers.



	Inputs	Assess	Outputs
Enterprise	• ICT SCRM Policy • Baseline Criticality	• Integrate ICT SCRM considerations into enterprise risk management	• ICT SCRM considerations integrated into enterprise risk management
Mission/Business Process	• ICT SCRM Mission/business requirements • Revised mission/business processes and enterprise architecture • ICT SCRM Risk Assessment Methodology • FIPS 199 impact levels • Mission Function Baseline Criticality • ICT SCRM Risk Assessment Methodology	• Conduct Risk Assessment including Criticality Analysis for mission threads • Determine current risk posture	• Mission function criticality • Mission risks • ICT supply chain risk assessment for mission threads
System	• System-level ICT SCRM requirements	• Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems • Determine current risk posture	• Identification of critical components • ICT supply chain risk assessment for individual systems

Figure 2-6: ICT SCRM in the Assess Step

Similar to Figure 2-5, Figure 2-6 depicts inputs, activities, and outputs of the Assess Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from other steps of the Risk Management Process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Assess Step include inputs from the other steps. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Criticality, vulnerability, and threat analyses are essential to the supply chain risk assessment process. As depicted in Figure 2-4, vulnerability and threat analyses can be performed in any order and may be performed iteratively to ensure that all applicable threats and vulnerabilities have been identified.

The order of activities that begins with the update of the criticality analysis ensures that the assessment is scoped to include only relevant critical mission functions and the impact of ICT supply chain on these mission functions. The likelihood of exploitability is a key step to understanding impact. It becomes a synthesis point for criticality analysis, vulnerability analysis, and threat analysis and helps to further clarify impact to support an efficient and cost-effective risk decision.

Activities

CRITICALITY ANALYSIS

TASK 2-0: Update Criticality Analysis of mission-critical functions, systems, and components to narrow the scope (and resources) for ICT SCRM activities to those most important to mission success.

Supplemental Guidance

Criticality analysis should include the ICT supply chain infrastructure for both the organization and applicable system integrators, suppliers, external service providers, and the systems/components/services. Criticality analysis assesses the direct impact they each have on the mission priorities. ICT supply chain infrastructure includes the SDLC for applicable systems, services, and components because the SDLC defines whether security considerations are built into the systems/components or added after systems/components have been created.

Organizations should update and tailor Baseline Criticality established during the Frame Step of the risk management process, including FIPS 199 system categorization, based on the information newly discovered in the Assess step. Organizations should use their own discretion for whether to perform criticality analysis for moderate-impact systems.

In addition to updating and tailoring Baseline Criticality, performing criticality analysis in the Assess Step may include the following:

- Perform a dependency analysis and assessment to establish which components may require hardening given the system architecture;
- Obtain and review existing information that the agency has about critical ICT systems/components such as locations where they are manufactured or developed, physical and logical delivery paths, information flows and financial transactions associated with these components, and any other available information that can provide insights into ICT supply chain of these components;[18] and
- Correlate identified critical components/services to the information about the ICT supply chain, the ICT supply chain infrastructure, historical data, and SDLC to identify critical ICT supply chain paths.

The outcome of the updated criticality analysis is a narrowed, prioritized list of the organization’s critical functions, systems, and components. Organizations can use the Baseline Criticality process in Chapter 2.2.1, Task 1-1, to update Criticality Analysis.

[18] This information may be available from a supply chain map for the agency or individual IT projects or systems. Supply chain maps are descriptions or depictions of supply chains including the physical and logical flow of goods, information, processes, and money upstream and downstream through a supply chain. They may include supply chain nodes, locations, delivery paths, or transactions.

Because more information will be available in the Assess step, organizations can narrow the scope and increase the granularity of a criticality analysis. When identifying critical functions and associated systems/components and assigning them criticality levels, consider the following:

- Functional breakdown is an effective method to identify functions, associated critical components, and supporting defensive functions;
- Dependency analysis is used to identify the functions on which critical functions depend (e.g., defensive functions such as digital signatures used in software patch acceptance). Those functions become critical functions themselves;
- Identification of all access points to identify and limit unmediated access to critical function/components (e.g., least-privilege implementation); and
- Malicious alteration can happen throughout the SDLC.

The resulting list of critical functions is used to guide and inform the vulnerability analysis and threat analysis to determine the initial ICT SCRM risk as depicted in Figure 2-3. ICT supply chain countermeasures and mitigations can then be selected and implemented to reduce risk to acceptable levels.

Criticality analysis is performed iteratively and may be performed at any point in the SDLC and concurrently at each tier. The first iteration is likely to identify critical functions and systems/components that have a direct impact on mission functions. Successive iterations will include information from the criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies defined at each of the other tiers. Each iteration will refine the criticality analysis outcomes and result in the addition of defensive functions. Several iterations are likely needed to establish and maintain the criticality analysis results.

THREAT AND VULNERABILITY IDENTIFICATION

TASK 2-1: Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.

Supplemental Guidance

In addition to threat and vulnerability identification, as described in [NIST SP 800-39] and [NIST SP 800-30 Rev. 1], organizations should conduct ICT supply chain threat analysis and vulnerability analysis.

Threat Analysis

For ICT SCRM, a threat analysis provides specific and timely threat characterization of threat events (see Appendix C) and potential threat actors, including any identified system integrators, suppliers, or external service providers,[19] to inform management, acquisition, engineering, and operational activities within an

[19] Please note that threat characterization of system integrators, suppliers, and external service providers may be benign.

organization. Threat analyses can use a variety of information to assess potential threats, including open source, intelligence, and counterintelligence. Organizations should use the threat sources defined during the Frame Step in the threat analysis conducted during the Assess Step. Organizations should use the results of the threat analysis in the Assess Step to ultimately support acquisition decisions, alternative build decisions, and development and selection of appropriate mitigations in the Respond Step. ICT supply chain threat analysis should be based on the results of the criticality analysis. Specific identified threats may include people, processes, technologies, or natural and man-made disasters.

Agencies should use information available from existing incident management activities to determine whether they have experienced an ICT supply chain compromise and to further investigate such compromises. Some ICT supply chain compromises may not be recognized as such at first and may be initially identified as an information security or logistics incident. Agencies should define criteria for what constitutes an ICT supply chain compromise to ensure that such compromises can be identified as a part of post-incident activities, including forensics investigations.

An ICT supply chain threat analysis should capture at least the following data:

- Changes to the systems/components or SDLC environment;
- Observation of ICT supply chain-related attacks while they are occurring;
- Incident data collected post-ICT supply chain-related compromise;
- Observation of tactics, techniques, and procedures used in specific attacks, whether observed or collected using audit mechanisms; and
- Natural and man-made disasters before, during, and after occurrence.

Vulnerability Analysis

For ICT SCRM, a vulnerability is any weakness in system/component design, development, production, or operation that can be exploited by a threat to defeat a system’s mission objectives or to significantly degrade its performance.

A vulnerability analysis is an iterative process that informs risk assessment and countermeasure selection. The vulnerability analysis works alongside the threat analysis to help inform the impact analysis and to help scope and prioritize vulnerabilities to be mitigated.

Vulnerability analysis in the Assess Step should use the approaches used during the Frame Step to characterize ICT supply chain vulnerabilities. Vulnerability analysis should begin with identifying vulnerabilities that are applicable to mission-critical functions and systems/components identified by the criticality analysis. An investigation of vulnerabilities may indicate the need to raise or at least reconsider the criticality levels of functions and components identified in earlier criticality analyses. Later iterations of the vulnerability analysis may also identify additional threats, or opportunities for threats, not considered in earlier threat assessments.

Table 2-6 provides examples of applicable ICT supply chain vulnerabilities that can be observed within the three organizational tiers.

Table 2-6: Examples of ICT Supply Chain Vulnerabilities Mapped to the Organizational Tiers

	Vulnerability Types	Mitigation Types
Tier 1 – Organization	1) Deficiencies or weaknesses in organizational governance structures or processes such as a lack of ICT SCRM Plan	1) Provide guidance on how to consider dependencies on external organizations as vulnerabilities. 2) Seek out alternate sources of new technology including building in-house.
Tier 2 – Mission/ Business	1) No operational process is in place for detecting counterfeits. 2) No budget was allocated for the implementation of a technical screening for acceptance testing of ICT components entering the SDLC as replacement parts. 3) Susceptibility to adverse issues from innovative technology supply sources (e.g., technology owned or managed by third parties is buggy).	1) Develop a program for detecting counterfeits and allocate appropriate budgets for putting in resources and training. 2) Allocate budget for acceptance testing – technical screening of components entering into SDLC.
Tier 3 – Operation	1) Discrepancy in system functions not meeting requirements, resulting in substantial impact to performance,	1) Initiate engineering change. Malicious alteration can happen throughout the system life cycle to an agency system to address functional discrepancy and test correction for performance impact.

The principal vulnerabilities to identify are:

- Access paths within the supply chain that would allow malicious actors to gain information about the system and ultimately introduce components that could cause the system to fail at some later time (“components” here include hardware, software, and firmware);
- Access paths that would allow malicious actors to trigger a component malfunction or failure during system operations; and
- Dependencies on supporting or associated components that might be more accessible or easier for malicious actors to subvert than components that directly perform critical functions.

RISK DETERMINATION

TASK 2-2: Determine the risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities.

Supplemental Guidance

Organizations determine ICT supply chain risk by considering the likelihood that known threats exploit known vulnerabilities to and through the ICT supply chain and the resulting consequences or adverse impacts (i.e., magnitude of harm) if such exploitations occur. Organizations use threat and vulnerability information together with likelihood and consequences/impact information to determine ICT SCRM risk either qualitatively or quantitatively.

Likelihood

Likelihood is the probability that an exploit occurrence may result in the loss of mission capability. Determining the likelihood requires the consideration of the characteristics of the threat sources, the identified vulnerabilities, and the organizations susceptibility to the ICT supply chain compromise, prior to and with the safeguards/mitigations implemented. This analysis should consider the degree of an adversary's intent to interfere with the organization's mission. For example, how much time or money would the adversary spend to validate the existence of and leverage the vulnerability to attack a system? ICT supply chain risk assessment should consider two views:

- The likelihood that the ICT supply chain itself is compromised. This may impact, for example, the availability of quality components or increase the risk of intellectual property theft; and
- The likelihood that the system or component within the supply chain may be compromised, for example, if malicious code is inserted into a system or an electric storm damages a component.

In some cases, these two views may overlap or be indistinguishable, but both may have an impact on the agency's ability to perform its mission.

Likelihood determination should consider:

- Threat assumptions that articulate the types of threats that the system or the component may be subject to, such as cybersecurity threats, natural disasters, or physical security threats;
- Actual supply chain threat information such as adversaries' capabilities, tools, intentions, and targets;
- Exposure of components to external access;
- Identified system, process, or component vulnerabilities; and
- Empirical data on weaknesses and vulnerabilities available from any completed analysis (e.g., system analysis, process analysis) to determine probabilities of ICT supply chain threat occurrence.

Factors to consider include the ease or difficulty of successfully attacking through a vulnerability and the ability to detect the method used to introduce or trigger a vulnerability. The objective is to assess the net effect of the vulnerability, which will be combined with threat information to determine the likelihood of successful attacks in the risk assessment process. The likelihood can be based on threat assumptions or actual threat data, such as previous breaches of the supply chain, specific adversary capability, historical breach trends, or frequency of breaches. The organization may use empirical data and statistical analysis to determine specific probabilities of breach occurrence, depending on the type of data available and accessible within the organization and from supporting organizations.

Impact

Organizations should begin impact analysis with the potential impacts identified during the Frame Step, determining the *impact* of a compromise and then the impact of mitigating that compromise. Organizations need to identify the various adverse impacts of compromise, including: (i) the characteristics of the threat sources that could initiate the events; (ii) identified vulnerabilities; and (iii) the organizational susceptibility to such events based on planned or implemented countermeasures. Impact analysis is an iterative process performed initially when a compromise occurs, when mitigation approach is decided to evaluate the impact of change, and finally, in the ever-changing SDLC, when the situation/context of the system or environment changes.

Organizations should use the result of impact analysis to define an acceptable level of ICT supply chain risk for a given system. Impact is derived from criticality, threat, and vulnerability analyses results, and should be based on the likelihood of exploit occurrence. Impact is likely to be a qualitative measure requiring analytic judgment. Executive/decision makers use impact as an input into the risk-based decisions whether to accept, avoid, mitigate, share, or transfer the resulting risks and the consequences of such decisions.

Organizations should document the overall results of ICT supply chain risk assessments in risk assessment reports.[20] ICT supply chain risk assessment reports should cover risks in all three organizational tiers as applicable. Based on the organizational structure and size, multiple ICT supply chain risk assessment reports may be required. Agencies are encouraged to develop individual reports at Tier 1. For Tier 2, agencies may want to integrate ICT supply chain risks into the respective mission-level Business Impact Assessments (BIA) or develop separate mission-level ICT supply chain risk assessment reports. For Tier 3, agencies may want to integrate ICT supply chain risks into the respective System Risk assessment reports or develop separate system-level ICT supply chain risk assessment reports. The ICT supply chain risk assessment report applies only to High Criticality systems per [FIPS 199]. Organizations may decide to develop ICT supply chain risk assessment reports for Moderate Criticality systems per [FIPS 199].

ICT supply chain risk assessment reports at all three tiers should be interconnected, reference each other when appropriate, and integrated into the ICT SCRM Plans.

Outputs and Post Conditions

This step results in:

- Confirmed mission function criticality;
- Establishment of relationships between the critical aspects of the system’s ICT supply chain infrastructure (e.g., SDLC) and applicable threats and vulnerabilities;
- Understanding of the likelihood and the impact of a potential ICT supply chain compromise;
- Understanding of mission and system-specific risks;
- Documented ICT supply chain risk assessments for mission functions and individual systems; and
- Integration of relevant ICT supply chain risk assessment results into the organization risk management process.

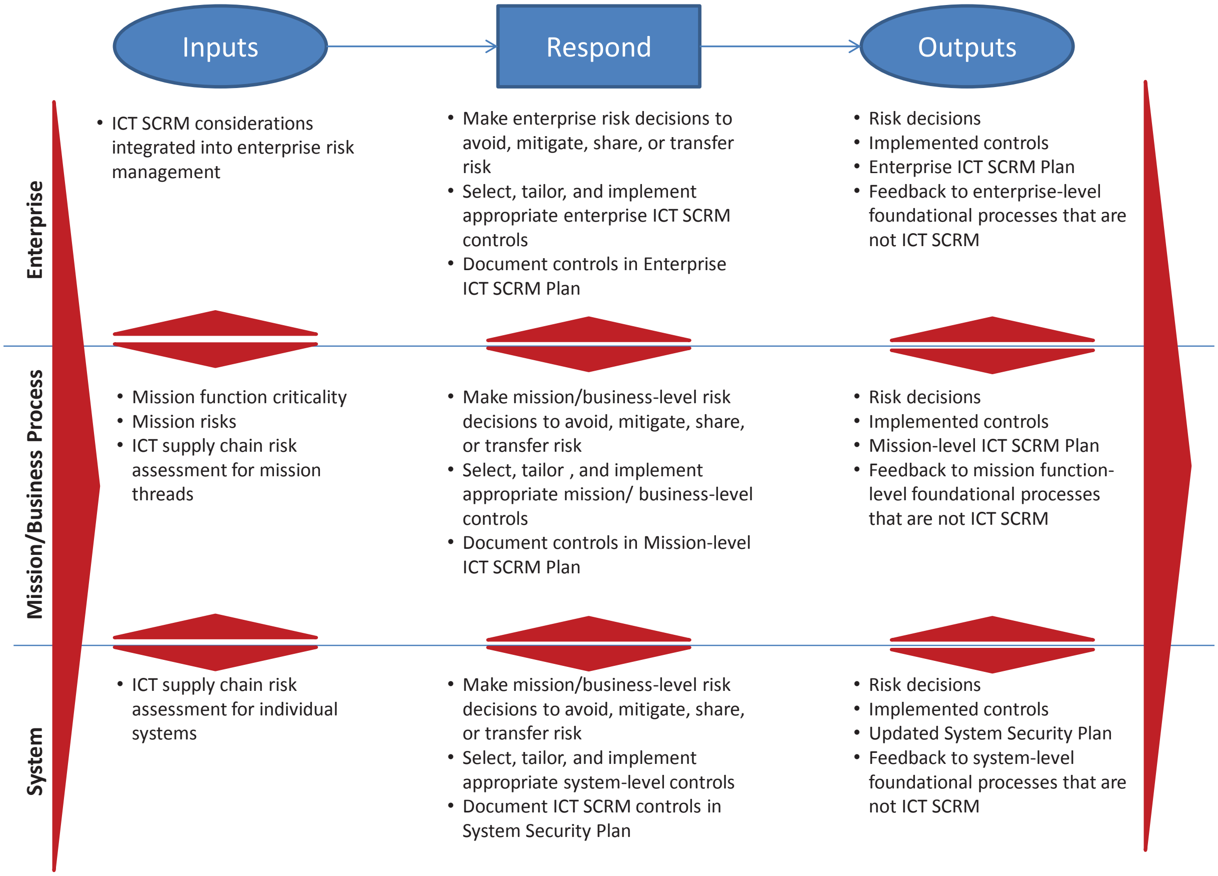
[20] See [NIST SP 800-30 Rev. 1 Appendix K] for a description of risk assessment reports.

2.2.3 RESPOND

Inputs and Preconditions

Respond is the step in which the individuals conducting risk assessment will communicate the assessment results, proposed mitigation/controls options, and the corresponding acceptable level of risk for each proposed option to the decision makers. This information should be presented in a manner appropriate to inform and guide risk-based decisions. This will allow decision makers to finalize appropriate risk response based on the set of options along with the corresponding risk factors for choosing the various options. Sometimes an appropriate response is to do nothing and to monitor the adversary's activities and behavior to better understand the tactics and to attribute the activities.

ICT supply chain risk response should be integrated into the overall organization risk response. Figure 2-7 depicts the Respond Step with its inputs and outputs along the three organizational tiers.



	Inputs	Respond	Outputs
Enterprise	• ICT SCRM considerations integrated into enterprise risk management	• Make enterprise risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor, and implement appropriate enterprise ICT SCRM controls • Document controls in Enterprise ICT SCRM Plan	• Risk decisions • Implemented controls • Enterprise ICT SCRM Plan • Feedback to enterprise-level foundational processes that are not ICT SCRM
Mission/Business Process	• Mission function criticality • Mission risks • ICT supply chain risk assessment for mission threads	• Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor , and implement appropriate mission/ business-level controls • Document controls in Mission-level ICT SCRM Plan	• Risk decisions • Implemented controls • Mission-level ICT SCRM Plan • Feedback to mission function-level foundational processes that are not ICT SCRM
System	• ICT supply chain risk assessment for individual systems	• Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor, and implement appropriate system-level controls • Document ICT SCRM controls in System Security Plan	• Risk decisions • Implemented controls • Updated System Security Plan • Feedback to system-level foundational processes that are not ICT SCRM

Figure 2-7: ICT SCRM in the Respond Step

Figure 2-7 depicts inputs, activities, and outputs of the Respond Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from the other steps of the Risk Management Process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Respond Step include inputs from other steps. Outputs of the Respond Steps serve as inputs into the other steps, as well as inputs into the overall organization Risk Management Program at all three tiers. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Activities

RISK RESPONSE IDENTIFICATION

TASK 3-1: Identify alternative courses of action to respond to risk determined during the risk assessment.

Organizations should select ICT SCRM controls and tailor these controls based on the risk determination. ICT SCRM controls should be selected for all three organizational tiers, as appropriate per findings of the risk assessments for each of the tiers.

Many of the ICT SCRM controls included in this document may be part of an IT security plan. These controls are included because they apply to ICT SCRM.

This process should begin with determining acceptable risk to support the evaluation of alternatives (also known as trade-off analysis).

EVALUATION OF ALTERNATIVES

TASK 3-2: Evaluate alternative courses of action for responding to risk.

Once an initial acceptable level of risk has been defined and options identified, these options should be evaluated for achieving this level of risk by selecting mitigations from ICT SCRM controls and tailoring them to the organization’s context. Chapter 3 provides risk mitigations and more information on how to select and tailor them.

This step involves conducting analysis of alternatives to select the proposed options for ICT SCRM mitigations/controls to be applied throughout the organization.

To tailor a set of ICT SCRM controls, the organization should perform ICT SCRM and mission-level trade-off analysis to achieve appropriate balance among ICT SCRM and functionality needs of the organization. This analysis will result in a set of cost-effective ICT SCRM controls that is dynamically updated to ensure that mission-related considerations trigger updates to ICT SCRM controls.

During this evaluation, applicable requirements and constraints are reviewed with the stakeholders to ensure that ICT SCRM controls appropriately balance ICT SCRM and the broader organizational requirements, such as cost, schedule, performance, policy, and compliance.

ICT SCRM controls will vary depending on where they are applied within organizational tiers and SDLC processes. For example, ICT SCRM controls may range from using a blind buying strategy to obscure end use of a critical component, to design attributes (e.g., input validation, sandboxes, and anti-tamper design). For each implemented control, the organization should identify someone responsible for its execution and develop a time- or event-phased plan for implementation throughout the SDLC. Multiple controls may address a wide range of possible risks. Therefore, understanding how the controls impact the overall risk is critical and must be considered before choosing and tailoring the combination of controls as yet another trade-off analysis may be needed before the controls can be finalized. The organization may be trading one risk for a larger risk unknowingly if the dependencies between the proposed controls and the overall risk are not understood and addressed.

RISK RESPONSE DECISION

TASK 3-3: Decide on the appropriate course of action for responding to risk.
As described in [NIST SP 800-39] , organizations should finalize identified and tailored ICT SCRM controls, based on the evaluation of alternatives and an overall understanding of threats, risks, and supply chain priorities.

Risk response decisions may be made by a risk executive or be delegated by the risk executive to someone else in the organization. While the decision can be delegated to Tier 2 or Tier 3, the significance and the reach of the impact should determine the tier where the decision is being made. Risk response decisions may be made in collaboration with an organization's risk executives, mission owners, and system owners, as appropriate.

The resulting decision, along with the selected and tailored controls should be documented in an ICT SCRM Plan. While the ICT SCRM Plan should ideally be developed proactively, it may also be developed in response to an ICT supply chain compromise. Ultimately, the ICT SCRM Plan should cover the full SDLC, document an ICT SCRM baseline, and identify ICT supply chain requirements and controls for Tiers 1, 2, and 3. The ICT SCRM Plan should be revised and updated based on the output of ICT supply chain monitoring.

ICT SCRM Plans should:

- Represent the result of an internal dialogue among Tiers 1, 2, and 3 stakeholders within the organization in support of the organization's mission and relevant mission function;
- Set the framework for an external dialogue between acquirers and system integrators, suppliers, and external service providers;
- Help define the state of the information system that will be "fit for purpose"; and
- Establish acceptance criteria that may be used in acquiring and sourcing ICT components and services.

The ICT SCRM Plan should cover activities in all three organizational tiers as applicable.

Depending on their governance structure and size, agencies can have multiple ICT SCRM Plans, one for Tier 1, several for Tier 2, and several for Tier 3. Agencies are encouraged to develop individual plans at Tiers 1 and 2. For Tier 3, agencies may want to integrate ICT SCRM controls into the respective System Security Plans or develop separate system-level ICT SCRM Plans. At Tier 3, the ICT SCRM Plan applies to High-Impact systems per [FIPS 199] , though organizations may decide to develop an ICT SCRM Plan for Moderate-Impact systems per [FIPS 199]. Regardless of the total number of plans, the ICT SCRM requirements and controls at the higher tiers will flow down to the lower tiers and should be used to guide the development of the lower tier ICT SCRM Plans. Conversely, the ICT SCRM controls and requirements at the lower tiers should be considered in developing and revising requirements and controls applied at the higher tiers. Agencies may choose to integrate their Tier 3 ICT SCRM controls into the applicable System Security Plans or create individual ICT SCRM Plans for Tier 3 that reference corresponding System Security Plans.

ICT SCRM Plans at all three tiers should be interconnected and reference each other when appropriate.

At each Tier, the plan should:

- Summarize the environment as determined in Frame such as applicable policies, processes, and procedures based on organization and mission requirements currently implemented in the organization;
- State the role responsible for the plan such as Risk Executive, Chief Financial Officer (CFO), Chief Information Officer (CIO), Program Manager, or System Owner;
- Identify key contributors such as CFO, Chief Operations Officer (COO), Acquisition/Contracting, System Engineer, System Security Engineer, Developer/Maintenance Engineer, Operations Manager, or System Architect;
- Provide the applicable (per tier) set of controls resulting from the Analysis of Alternatives (in Respond);
- Provide tailoring decision for selected controls including the rationale for the decision;
- Describe feedback processes among the tiers to ensure that ICT supply chain interdependencies are addressed;
- Describe monitoring and enforcement activities (including auditing if appropriate) applicable to the scope of each specific ICT SCRM Plan;
- If appropriate, state qualitative or quantitative measures to support implementation of the ICT SCRM Plan and to assess effectiveness of this implementation;[21]
- Define frequency for deciding whether the plan needs to be reviewed and revised;
- Include criteria that would trigger revision, for example, life cycle milestones, gate reviews, or significant contracting activities; and
- Include system integrator, supplier, and external service provider ICT SCRM Plans if made available as part of agreements.

Table 2-7 summarizes the controls to be contained in the ICT SCRM Plans at Tiers 1, 2, and 3 and provides examples of those controls.

[21] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security* (July 2008), provides guidance on developing information security measures. Agencies can use general guidance in that publication to develop specific measures for their ICT SCRM plans. See http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Table 2-7: ICT SCRM Plan Controls at Tiers 1, 2, and 3

Tier	Controls	Examples
Tier 1	• Provides organization common controls baseline to Tiers 2 and 3	• Minimum sets of controls applicable to all ICT suppliers • Organization-level controls applied to processing and storing supplier information • ICT supply chain training and awareness for acquirer staff at the organization level
Tier 2	• Inherits common controls from Tier 1 • Provides mission function-level common controls baseline to Tier 3 • Provides feedback to Tier 1 about what is working and what needs to be changed	• Minimum sets of controls applicable to ICT suppliers for the specific mission function • Program-level refinement of Identity and Access Management controls to address ICT SCRM concerns • Program-specific ICT supply chain training and awareness
Tier 3	• Inherits common controls from Tiers 1 and 2 • Provides system-specific controls for Tier 3 • Provides feedback to Tier 2 and Tier 1 about what is working and what needs to be changed	• Minimum sets of controls applicable to specific hardware and software for the individual system • Appropriately rigorous acceptance criteria for change management for systems that support ICT supply chain, e.g., as testing or integrated development environments • System-specific ICT supply chain training and awareness • Intersections with the SDLC

Appendix E provides an example ICT SCRM Plan template with the sections and the type of information that organizations should include in their ICT SCRM Planning activities.

RISK RESPONSE IMPLEMENTATION
TASK 3-4: Implement the course of action selected to respond to risk.

Organizations should implement the ICT SCRM Plan in a manner that integrates the ICT SCRM controls into the overall agency risk management processes.

Outputs and Post Conditions

The output of this step is a set of ICT SCRM controls that address ICT SCRM requirements and can be incorporated into the system requirements baseline. These requirements and resulting controls will be incorporated into the SDLC and other organizational processes, throughout the three tiers.

This step results in:

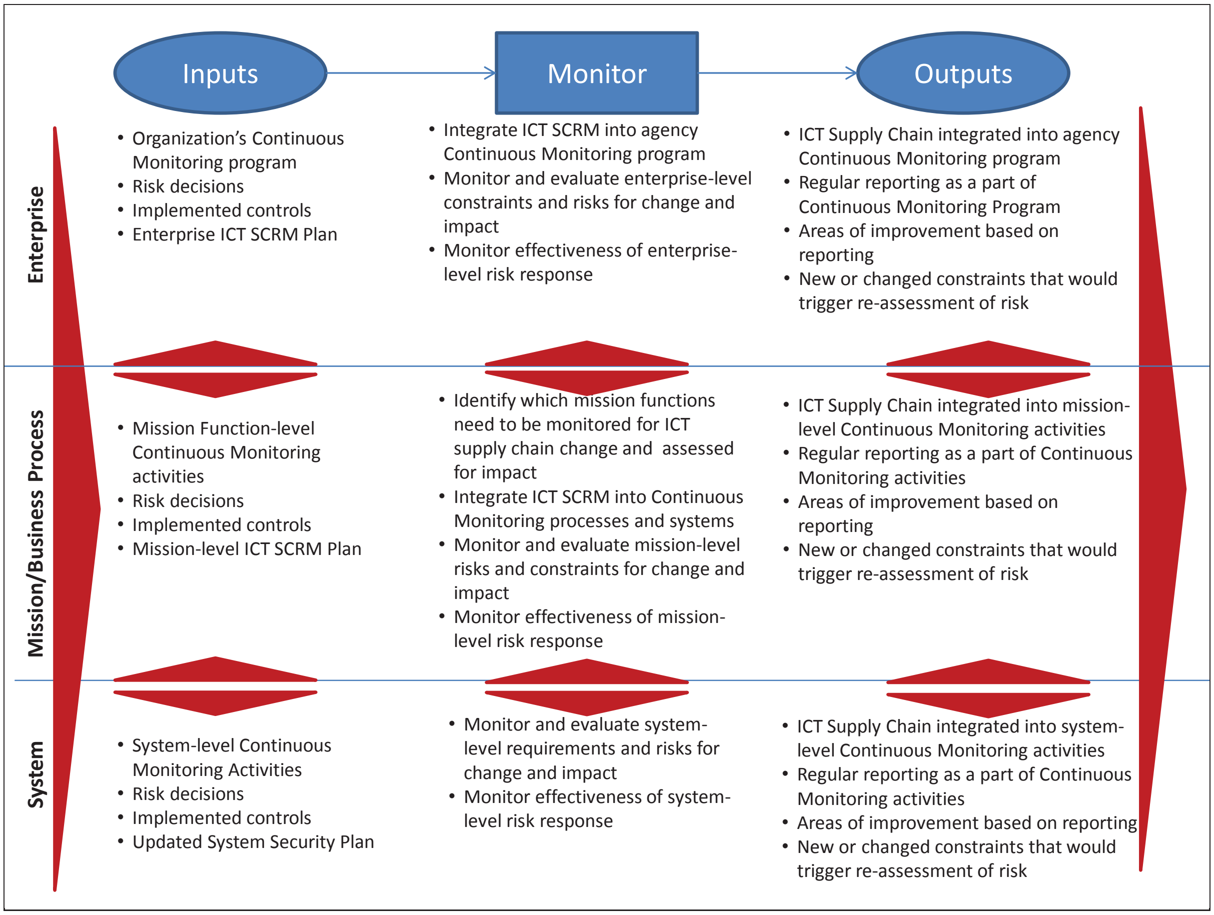
- Selected, evaluated, and tailored ICT SCRM controls that address identified risks;
- Identified consequences of accepting or not accepting the proposed mitigations; and
- Development and implementation of the ICT SCRM Plan.

2.2.4 MONITOR

Inputs and Preconditions

Monitor is the step in which the project/program is routinely evaluated to maintain or adjust the acceptable level of risk. Changes to the organization, mission/business, operations, or the supply chain can directly impact an individual project/program and the organization's ICT supply chain infrastructure. The monitor step provides a mechanism for tracking such changes and ensuring that they are appropriately assessed for impact (in Assess). If ICT supply chain infrastructure is redefined as a result of monitoring, organizations should engage in a dialog with the system integrators, supplier, and external service providers about implications and mutual obligations.

Organizations should integrate ICT SCRM into existing continuous monitoring programs.[22] In case a Continuous Monitoring program does not exist, ICT SCRM can serve as a catalyst for establishment of a more comprehensive continuous monitoring program. Figure 2-8 depicts the Monitor Step with its inputs and outputs along the three organizational tiers.



Enterprise – Inputs:

- Organization's Continuous Monitoring program
- Risk decisions
- Implemented controls
- Enterprise ICT SCRM Plan

Enterprise – Monitor:

- Integrate ICT SCRM into agency Continuous Monitoring program
- Monitor and evaluate enterprise-level constraints and risks for change and impact
- Monitor effectiveness of enterprise-level risk response

Enterprise – Outputs:

- ICT Supply Chain integrated into agency Continuous Monitoring program
- Regular reporting as a part of Continuous Monitoring Program
- Areas of improvement based on reporting
- New or changed constraints that would trigger re-assessment of risk

Mission/Business Process – Inputs:

- Mission Function-level Continuous Monitoring activities
- Risk decisions
- Implemented controls
- Mission-level ICT SCRM Plan

Mission/Business Process – Monitor:

- Identify which mission functions need to be monitored for ICT supply chain change and assessed for impact
- Integrate ICT SCRM into Continuous Monitoring processes and systems
- Monitor and evaluate mission-level risks and constraints for change and impact
- Monitor effectiveness of mission-level risk response

Mission/Business Process – Outputs:

- ICT Supply Chain integrated into mission-level Continuous Monitoring activities
- Regular reporting as a part of Continuous Monitoring activities
- Areas of improvement based on reporting
- New or changed constraints that would trigger re-assessment of risk

System – Inputs:

- System-level Continuous Monitoring Activities
- Risk decisions
- Implemented controls
- Updated System Security Plan

System – Monitor:

- Monitor and evaluate system-level requirements and risks for change and impact
- Monitor effectiveness of system-level risk response

System – Outputs:

- ICT Supply Chain integrated into system-level Continuous Monitoring activities
- Regular reporting as a part of Continuous Monitoring activities
- Areas of improvement based on reporting
- New or changed constraints that would trigger re-assessment of risk

Figure 2-8: ICT SCRM in the Monitor Step

[22] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011), describes how to establish and implement a continuous monitoring program. See http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Similarly to Figures 2-5, 2-6, and 2-7, Figure 2-8 depicts inputs, activities, and outputs of the Monitor Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from the other steps of the risk management process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Monitor Step include inputs from other steps, as well as from the organization Continuous Monitoring program and activities. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Activities

RISK MONITORING STRATEGY

TASK 4-1: Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.

Supplemental Guidance:

Organizations should integrate ICT SCRM considerations into their overall risk monitoring strategy. Because some of the information will be gathered from outside of the agency – from open sources, suppliers and integrators, monitoring ICT supply chain risk may require information that agencies have not traditionally collected. The strategy should, among other things, include the data to be collected, state the specific measures that will be compiled from the data, identify existing or required tools to collect the data, identify how the data will be protected, and define reporting formats for the data. Potential data sources may include:

- Agency vulnerability management and incident management activities;
- Agency manual reviews;
- Interagency information sharing;
- Information sharing between the agency and system integrator or external service provider;
- Supplier information sharing; and
- Contractual reviews of system integrator or external service provider.

Organizations should ensure the appropriate protection of supplier data if that data is collected and stored by the agency. Agencies may also require additional data collection and analysis tools to appropriately evaluate the data to achieve the objective of monitoring applicable ICT supply chain risks.

RISK MONITORING

TASK 4-2: Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

According to [NIST SP 800-39], organizations should monitor compliance, effectiveness, and change. Monitoring compliance within the context of ICT SCRM involves monitoring an organization’s processes and ICT products and services for compliance with the established security and ICT SCRM requirements. Monitoring effectiveness involves monitoring the resulting risks to determine whether these established security and ICT SCRM requirements produce the intended results. Monitoring change involves monitoring the environment for any changes that would require changing requirements and mitigations/controls to maintain an acceptable level of ICT supply chain risk.

To monitor changes, organizations need to identify and document the set of triggers that would change ICT supply chain risk. While the categories of triggers will likely include changes to constraints, identified in Table 2-6 (during the Frame Step), such as policy, mission, change to the threat environment, enterprise architecture, SDLC, or requirements, the specific triggers within those categories may be substantially different for different organizations.

An example of the ICT supply chain infrastructure change is two key vetted suppliers[23] announcing their departure from a specific market, therefore creating a supply shortage for specific components. This would trigger the need to evaluate whether reducing the number of suppliers would create vulnerabilities in component availability and integrity. In this scenario, potential deficit of components may result simply from insufficient supply of components, because fewer components are available. If none of the remaining suppliers are vetted, this deficit may result in uncertain integrity of the remaining components. If the organizational policy directs use of vetted components, this event may result in the organization's inability to fulfill its mission needs.

In addition to regularly updating existing risks assessments with the results of the ongoing monitoring, the organization should determine what would trigger a reassessment. Some of these triggers may include availability of resources, changes to ICT supply chain risk, natural disasters, or mission collapse.

Outputs and Post Conditions

Organizations should integrate the ICT supply chain outputs of the Monitor Step into the ICT SCRM Plan. This plan will provide inputs into iterative implementations of the Frame, Assess, and Respond Steps as required.

[23] A vetted supplier is a supplier with whom the organization is comfortable doing business. This level of comfort is usually achieved through developing an organization-defined set of supply chain criteria and then *vetting* suppliers against those criteria.