Supply Chain Security

Lecture 13
Dec, 2014

1

ICT Supply Chain

- Complex, Global, Distributed, Interconnected Networks
  - Organizations, processes, products, services and infrastructure
  - Today's: Significant Complexity, Diversity and Scale
- System integrators
  - distinct role of assembling information systems, system components, and information services

Example:
Target breach – HVAC company

Global supply chain is the "the next playground for hackers,"
(International Maritime Bureau (IMB))

Gartner Says IT Supply Chain Integrity Will Be Identified as a Top Three Security-Related Concern by Global 2000 IT Leaders by 2017

Supply Chain Risk

- ICT supply chain risks include
  - insertion of counterfeits, tampering, theft, and insertion of malicious software.
- Risks through exploits of vulnerabilities
  - Reduced functionality: poor or counterfeit components
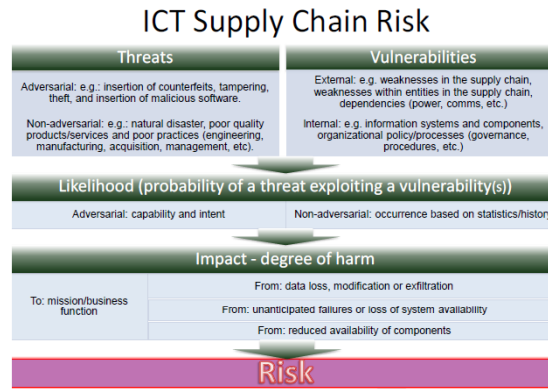 - Unwanted functionality: malware inserted, poor quality

ICT Supply Chain Risk

Threats	Vulnerabilities
Adversarial: e.g.: insertion of counterfeits, tampering, theft, and insertion of malicious software.	External: e.g. weaknesses in the supply chain, weaknesses within entities in the supply chain, dependencies (power, comms, etc.)
Non-adversarial: e.g.: natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, 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 1-1. ICT Supply Chain Risk

SC and Globalization

- Adversary may include: Individuals, Orgs, Nation-states
  - Directly or indirectly affect management and operations of companies; E.g.,
    - foreign nation states may force (i) a manufacturer to hand over spec of sensitive US system (ii) insert malware
- Need to protect information that
  - describes the ICT supply chain (e.g., information about the paths of ICT products and services, both logical and physical),
  - traverses the ICT supply chain (e.g., intellectual property contained in ICT products and services), and
  - information about the parties participating in the ICT supply chain (anyone who touches an ICT product or service throughout its life cycle).

Integrate SC with RM

- *Frame risk* – establish the context for risk-based decisions and the current state of the system or ICT supply chain environment;
- *Assess risk* – review and interpret threat, vulnerability, and related information;

- *Respond to risk once determined* – select, tailor, and implement mitigation controls; and,
- *Monitor risk* on an ongoing basis, including changes to an information system or ICT supply chain environment,
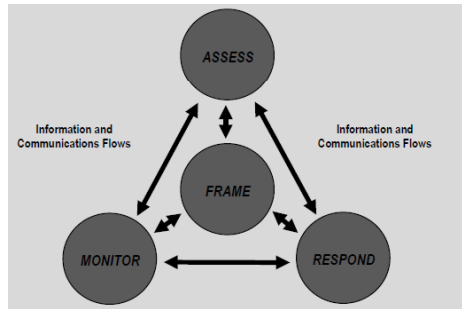

Table 2-1: Supply Chain Risk Management Stakeholders

Tiers	Tier Name	Generic Stakeholder	Activities
1	Organization	Executive Leadership (CEO, CIO, COO, CFO, CISO, CTO, etc.) - Risk executive	Corporate Strategy, Policy, goals and strategies

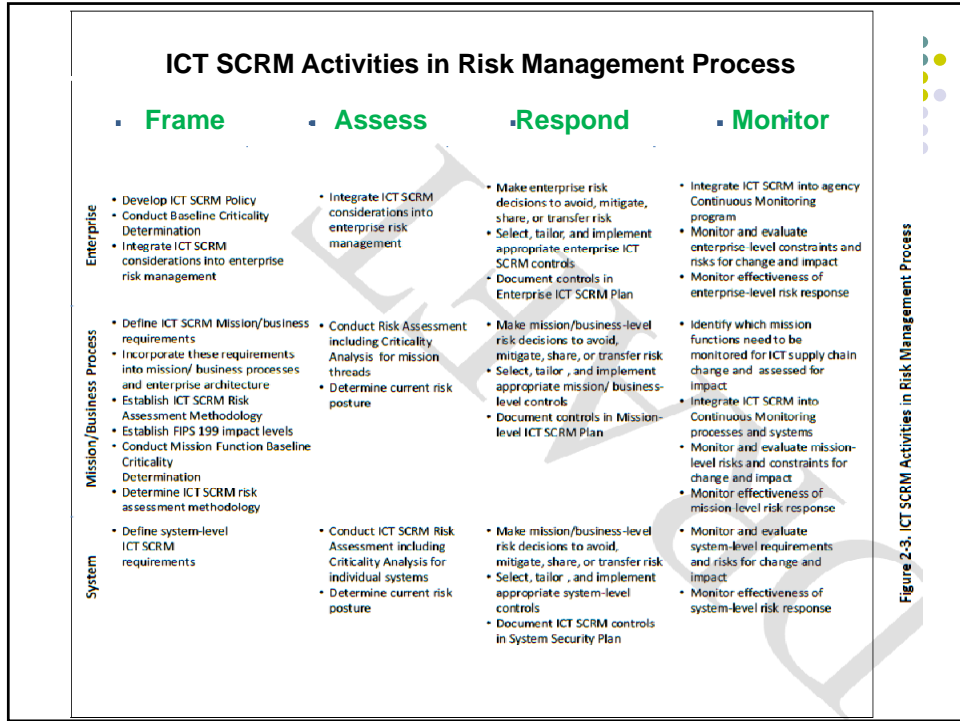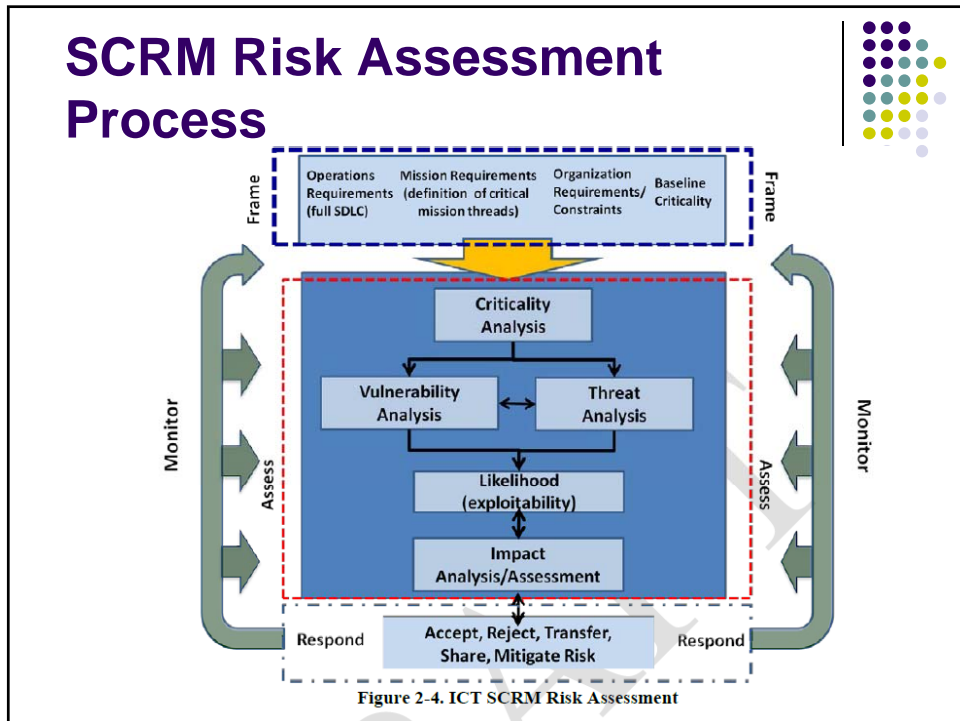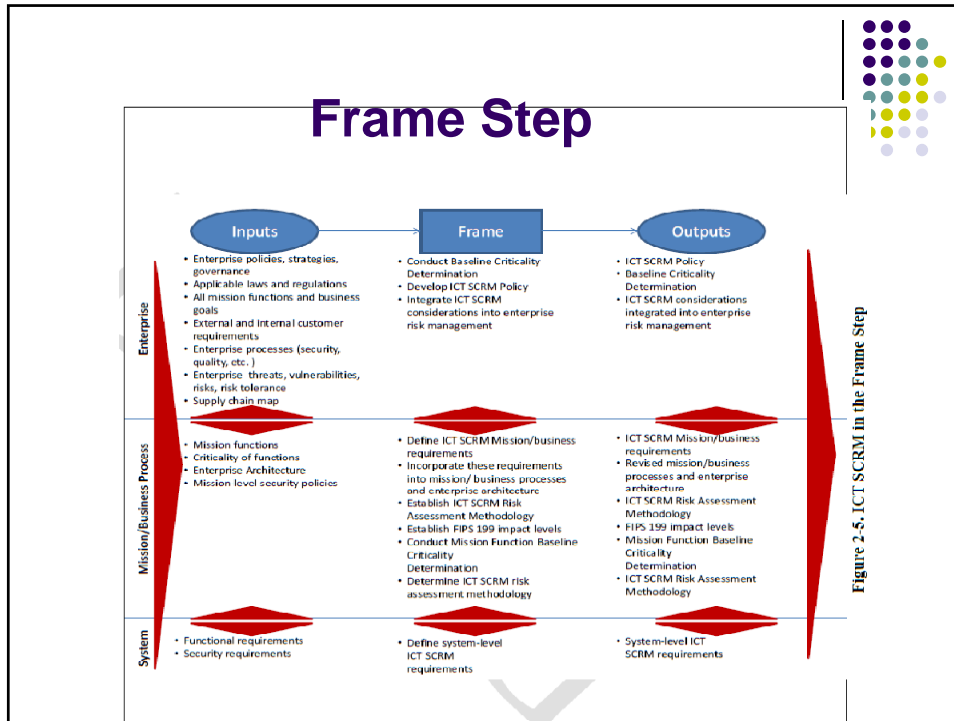| Tiers	Tier Name	Generic Stakeholder	Activities
2	Mission	Business Management (includes program management (PM), research and development (R&D), Engineering [SDLC oversight], Acquisitions / Procurement, Cost Accounting, - "ility" management [reliability, safety, quality], etc.)	Actionable Policies and procedures, Guidance and constraints
3	Operation	Systems Management (architect, developers, QA/QC, test, contracting personnel (approving selection, payment and approach for obtaining, maintenance engineering, disposal personnel, etc.)	Policy implementation Requirements, constraints implementations

ICT SCRM Activities in Risk Management Process

Frame   **Assess**   **Respond**   **Monitor**

Enterprise

Frame	Assess	Respond	Monitor
• 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

Frame	Assess	Respond	Monitor
• 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

Frame	Assess	Respond	Monitor
• 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 2-3. ICT SCRM Activities in Risk Management Process

SCRM Risk Assessment Process

Figure 2-4. ICT SCRM Risk Assessment

Frame Step

Figure 2-5. ICT SCRM in the Frame Step

Threat Agents

Threat Agent	Scenario	Examples
Counterfeiters	Counterfeits inserted into ICT supply chain (see Appendix F 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.[11]
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.[12]
Foreign Intelligence Services	Malicious code insertion (see Appendix F Scenario 3)	Foreign intelligence services seek to penetrate ICT supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) to be used when the system is operational to gather information or subvert system or mission operations.
Terrorists	Unauthorized access	Terrorists seek to penetrate ICT supply chain and may implant unwanted functionality (by inserting new or modifying existing functionality) or subvert system or mission operations.
Industrial Espionage	Industrial Espionage (see Appendix F Scenario 2)	Industrial spies seek to penetrate ICT supply chain to gather information or subvert system or mission operations.

Threat Considerations

Table 2-5. 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 natural disasters.
Tier 2	• Mission functions • Geographic locations • Types of suppliers (COTS, external service providers, or custom, etc.) • Technologies used enterprise-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 the agency supply chain map.
		• Scope identified threat sources to the specific mission functions, using the supply chain maps. • Establish mission-specific preparatory procedures for countering threat adversaries/natural disasters.
Tier 3	• SDLC	• Consider the phase in the system development life cycle to determine the level of detail with which threats should be considered. • Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes.

Vulnerabilities

Table 2-6. Supply Chain Vulnerabilities Considerations

Tier	Vulnerability Consideration	Methods

Tier 1	• Organization's business and mission
	• 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 Supply Chain Maps and/or historical data 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 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 CVEs to characterize and categorize vulnerabilities. • 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 of SC threats

- Examples of SC Consequences and Impact:
  - An earthquake in Malaysia reduced the number of commodity DRAMs to 60% 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, therefore impacting organization's mission performance.
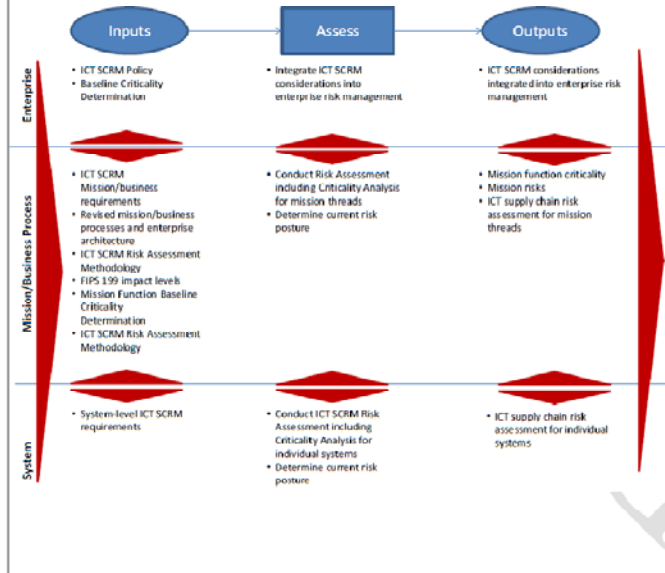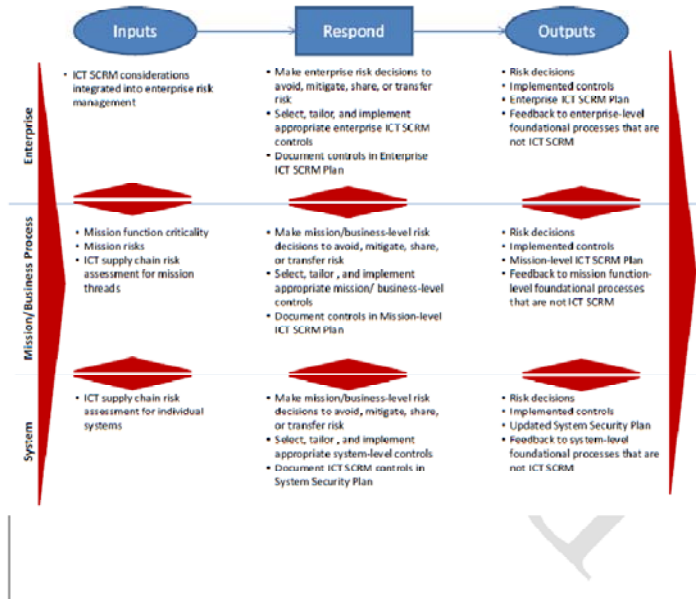
Integration with RM

- Need to identify: Agency constraints and SC-specific constraints

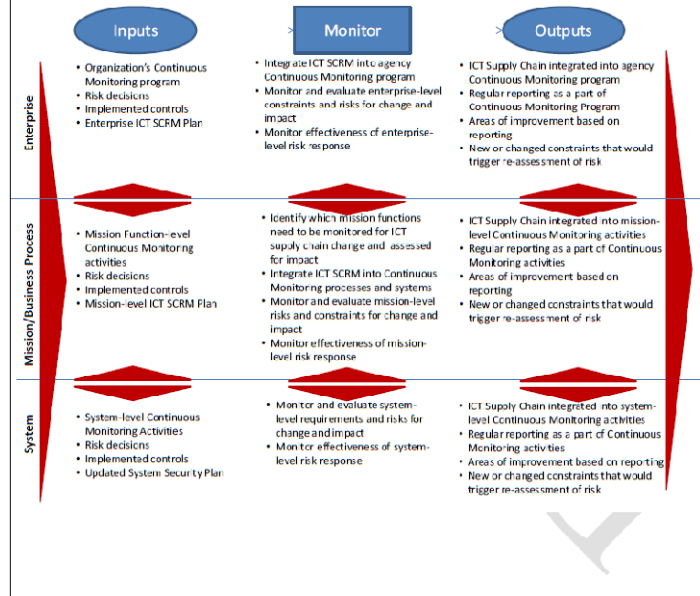| Tier	Agency Constraint	ICT Supply Chain Constraint
Tier 1	• Enterprise policies, strategies, governance • Applicable laws and regulations • Mission functions • Enterprise processes (security, quality, etc.)	• Develop enterprise ICT SCRM policy based on the existing agency policies, strategies, and governance; applicable laws and regulations; mission functions; and enterprise processes.
Tier 2	• 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.
Tier 3	• Functional requirements • Security requirements	• Define system-level ICT SCRM requirements.

Assess Step

Respond Step

Monitor Step

Inputs	Monitor	Outputs

Enterprise
- Inputs:
  - Organization's Continuous Monitoring program
  - Risk decisions
  - Implemented controls
  - Enterprise ICT SCRM Plan
- 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
- 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
- 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
- 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
- Monitor:
  - Monitor and evaluate system-level requirements and risks for change and impact
  - Monitor effectiveness of system-level risk response
- 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

---

SC Environment

- System Integrators
  - organizations that provide customized services to an acquirer - custom development, test, and operations and maintenance; may include many suppliers
- Suppliers
  - organizations providing commercial off-the-shelf (COTS) to an acquirer External Providers of InfoSys Services
  - Outsourcing IT services –

  - Visibility and control of functionality and security controls are critical

Summary

- Supply Chain Risk Management is critical to ensuring the overall system security
- Proper integration of SCRM within the organizational RM is important
- Three tiers of organizational risk management need to be adopted for SCRM