THE ICT SCRM COMMUNITY FRAMEWORK DEVELOPMENT PROJECT

FINAL REPORT

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

The Supply Chain Management Center
Robert H. Smith School Of Business
University of Maryland College Park

Principal Investigator: Dr. Sandor Boyson
Senior Advisors: Hart Rossman, Taylor Wilkerson

Acknowledgements

The authors would like to thank Jon Boyens for his collaborative spirit and strong support of this project; Dan Reddy for his invaluable industry insights and wisdom; Naveed Haghani and Ankit Agarwal for their research support; and Lori Newman for her design assistance.

We also want to thank all the industry and government members of the focus group for giving us the gift of their time.

Executive Summary

Under Initiative 11 of the President's CNCI Program, the National Institute of Standards and Technology (NIST) has been tasked with supporting federal policy development in Supply Chain Risk Management (SCRM) for Information Communications Technology (ICT).

To support NIST's work, the Supply Chain Management Center of the Robert H. Smith School of Business at the University of Maryland College Park was awarded a grant in August, 2011. Our project attempted to inventory the proliferating array of existing industry and public sector initiatives across diverse ICT segments (software, hardware, networks and system integration services).

It also formulated a ICT SCRM community framework capable of embracing the processes and practices defined in these various initiatives within a single risk management architecture. This framework has three tiers: enterprise risk governance, system integration and operations. Within each tier, we defined a core set of attributes or distinct organizational capabilities.

This framework conferred two broad capabilities: defense in breadth and defense in depth and was intended to enable each of the initiatives to better understand its own relative positioning in the ICT SCRM ecosystem; to highlight distinctive capabilities of and complementarities between initiatives; and to facilitate the identification and assessment of gaps in coverage in the ICT SCRM community.

We organized a focus group of participants from major organizations to review our initial approach and provide feedback. The newness of the discipline was a strong theme expressed by participants. When asked to rate the maturity of the ICT SCRM industry, twelve of nineteen respondents rated the industry as immature; and seven as somewhat mature. No one rated the industry as mature.

Finally, we asked participants to define the attractiveness of future options to build out the community framework. The preferred options were an independent public/ private partnership model to spur further community development (which received nine votes of nineteen cast); and NIST creating a Council of Initiatives (which received seven votes). Thus, 16 of 19 votes cast were for a collaborative government/industry model.

The need for a more defined public/private partnership in this space has also been expressed as a call to action by the National Science and Technology Council: "The national interest in some emerging areas of standardization such as **cyber security demands a new level of coordination and effort, and will require the development of new ways for the public and private sectors, as well as large numbers of standards development organizations and consortia, to work together in order to preserve national competitiveness."** *(Source: "Federal Engagement in Standards Activities to Address National Priorities: Background and Proposed Policy Recommendations", Subcommittee on Standards, National Science and Technology Council, October 2011, p.1).*

To support community development, NIST should consider these next steps:

- Develop a charter and governance structure for a public/private consortium to address ICT SCRM.
- Provide facilitation and analytical support for the consortium.
- Perform a more detailed mapping of initiatives to clearly identify gaps in current and planned activities and recommend areas that NIST can address to create a more comprehensive ICT SCRM ecosystem.
- Perform a more detailed mapping to identify inconsistencies in ICT SCRM approaches that NIST can help reconcile.
- Develop a guidance document for using multiple frameworks/standards to develop a comprehensive ICT SCRM program.
- Develop a maturity model that specifically takes an organization from annual self-assessments into quarterly supply chain reviews progressing to monthly sense/detect sessions and eventually to continuous monitoring of defense in depth & defense in breadth.
- Develop a methodology and toolset to support self-assessment.
- Create a technical support group for assisting the cyber supply chain community to evaluate practices and standards.

To Conclude: Our core research finding is that a wide swathe of the ICT SCRM community believes NIST has a pivotal role to play in accelerating the growth and maturity of community practices and standards.

The ICT SCRM Community Framework Development Project

TABLE OF CONTENTS

The ICT SCRM Community Framework Development Project

I. Project Background

Under Initiative 11 of the President's CNCI Program, the National Institute of Standards and Technology (NIST) has been tasked with integrating lessons learned from various federal and industry initiatives into guidance for the federal enterprise and its industry vendor/partners in the area of Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM).

To support NIST's ICT SCRM guideline development activities and NIST-IR publication, the Supply Chain Management Center of the RH Smith School of Business at the University of Maryland in College Park was awarded a grant in August, 2011. This grant attempted to inventory the proliferating array of existing industry and public sector initiatives; and to formulate a ICT SCRM Community Framework capable of embracing the processes and practices defined in these various initiatives within a single risk management architecture. This grant built upon the work already completed by the Supply Chain Management Center for NIST in winter/spring 2011 which provided a detailed profile of 200 of the federal government's key ICT vendors' supply chain risk governance strategies and practices.

We intend for this activity to help overcome functional area specialization/ fragmentation within the ICT industry supply chain risk management community. A ICT SCRM Community Framework can enable each of the initiatives to better understand its own relative positioning in the ICT SCRM ecosystem; to highlight distinctive capabilities of and complementarities between initiatives; and facilitate the identification and assessment of gaps in coverage in the ICT SCRM Community.

Finally, it can help build a larger sense of community and purpose by bringing together diverse stakeholders from across the ICT SCRM segments (software, hardware, networks, system integration services, etc) to address the overriding industry challenges of survival and growth.

The need for a more defined sense of public/private partnership and greater sense of community in this space has been highlighted as a call to action by the National Science and Technology Council:

"The national interest in some emerging areas of standardization such as homeland security, smart grid, healthcare, energy efficiency, nanotechnology, and **cybersecurity demands a new level of coordination and effort, and will require the development of new ways for the public and private sectors, as well as large numbers of standards development organizations and consortia, to work together in order to preserve national competitiveness.**"

(Source: "Federal Engagement in Standards Activities to Address National Priorities: Background and Proposed Policy Recommendations", Subcommittee on Standards, National Science and Technology Council, October 2011, p.1).

II. Project Design

A. Methodology For Creating A Reference Community Framework

At present, no readily identifiable large-scale end-to-end risk management model exists that cuts across the various functional areas of the ICT supply chain. Specialized bodies of knowledge have been created by various industry groupings that separately cover software, hardware, telcom network and systems-integration functions. There is a compelling need to conceptually integrate these separate functional area bodies of knowledge; identify the supply chain handoffs/interdependencies between them; and overlay the entire end to end process with a risk governance layer.

To assist in this effort, researchers referred to three key sources to create a comprehensive integrative framework:

- The Cyber Supply Chain Assurance Reference Model developed over a three year period by the Smith Supply Chain Management Center and SAIC which created a three ring nested model with an inner governance ring, a systems-integration ring and a field layer or action ring.
- The Supply Chain Operations Reference Model (SCOR®), which is the major industry reference model created in 1996 by the Supply Chain Council, and currently in use by over 800 companies. This model defines a set of enterprise risk management activities and process-level tasks encompassing the plan, source, make, deliver, return functions of the supply chain.
- The NIST Systems Development Lifecycle which includes the integration of security into each of its phases, from acquisition to disposition. This holistic approach supports the risk management methodology and provides comprehensive technical controls for auditing.

We created a Community Framework that incorporated these key elements into a three tiered ICT SCRM architecture with enterprise risk governance, system integration and operations tiers. Within each tier, we defined a core set of attributes or distinct organizational capabilities that comprise each tier.

This Framework conferred two broad capabilities: defense in breadth and defense in depth.

Defense in breath is extensive: it covers the whole end to end ecosystem of customer/acquirers, integrators, suppliers and key processes between them.

Defense in depth is intensive: it covers risk governance; systems lifecycle management including design, risk assessment and supply base modeling/auditing; and operations management.

These two capabilities together provide comprehensive ICT SCRM controls.

This integrative Framework was employed as a base process mapping tool to conduct ICT SCRM ecosystem modeling. Having established the tiers of the Framework and associated attributes for each tier, we then mapped the coverage areas of major ICT SCRM initiatives against the Framework. We worked with NIST to identify organizations operating in this space and collected documents in regards to their ICT SCRM initiatives.

Our team also developed a coding system to analyze and categorize document content based on how frequently and extensively each document "explicitly mentions"/addresses our Reference Framework ICT SCRM tiers and attributes within those tiers. We assigned one of three ratings to describe the level of an initiative's coverage of the core attributes associated with each of the tiers of the Framework; these ratings are represented as Harvey Balls that show circles with shaded areas representing extent of coverage-from minimal coverage to full coverage.

The ICT SCRM community is highly dynamic in reality, but in our initial research, it was largely a static representation gleaned through review of limited documentation and sometimes restricted web access to these organizations. We regarded this phase as a flawed but promising attempt to code these collective efforts; a start to bring the rich and diverse activities of the ICT SCRM community into a sharper focus.

To create a more vibrant and multidimensional representation, we organized a focus group at the University of Maryland College Park campus to review our initial approach and provide feedback. We invited the major organizations that we had mapped and coded to join this group as well as a sampling of ICT SCRM stakeholders.

B. The ICT SCRM Focus Group

The focus group was held on October 20, 2011 from 10 am to 3 pm at the Robert H. Smith School of Business, University of Maryland, College Park.

The declared purpose of the meeting was to gain community feedback on the ICT SCRM Community Framework and its set of associated attributes; and to lay out a first mapping of ICT SCRM initiatives within this Framework for discussion/modification.

Participants were asked to prepare for the focus group by reviewing the following four documents:

- The Strategic Positioning Graph, which showed a preliminary high level mapping of initiatives within the ICT SCRM Community, which was intended to stimulate discussion. Participants were asked to review this mapping for accuracy and modify their organization's positioning accordingly.
- The Process Positioning Graph, which was blank and was used in the meeting to focus in on priority supply chain and systems lifecycle processes covered by each initiative. We asked participants to consider where his/her own organization should be positioned on this graph.
- The Summary of Initiative Attributes which compared each initiative along multiple dimensions, or attributes. Each initiative was assigned a simple three point rating score based on the extent to which available documentation appeared to address a specific attribute. We asked participants to review his/her own organization's ratings for accuracy and modify accordingly.
- The Detailed Matrix Of Initiatives which described in more depth each of the major initiatives we catalogued for this exercise. We asked for feed back as to the accuracy and completeness of each initiative's detailed description.

Participating organizations and their representatives included:

DHS: Willie Garrett , Keith Hill (Mitre), Ross Gaiser

DOD: Rama Moorthy, Forrest Frank

FCC: Jeff Goldthorp, Jane Kelly

Intel: Audrey Plonk, John Miller

Internet Security Alliance: Joshua Magri

ISO 27036: Nadya Bartol (Booz Allen)

Microsoft: Tyson Storch

NIST: Jon Boyens, Celia Paulsen

NSA: Barry W. Guckes, Dorian Pappas, Eustace King

Open Group: Dan Reddy (EMC), Don Davidson (DOD)

SCOR/Supply Chain Council: J. Caspar Hunsche (SCC), Taylor Wilkerson (SCC/LMI/UMD)

UMD: Sandy Boyson, Hart Rossman, Mary Maxson, Naveed Haghani, Ankit Agarwal

The focus group schedule was composed of four modules, as follows:

Module 1: Conducted a baseline survey of respondents using electronic survey technology that received polling answers from respondents and collated the results in real time.

Module 2: Presented Tiers and Attributes of the Reference Framework we had developed and each Tier and Attribute was set out for electronic polling, with respondents asked to evaluate their usefulness.

Module 3: Presented the initial outputs of our Community Mapping Exercise and we set out these results for electronic polling as well.

Module 4: Defined and voted on next steps.

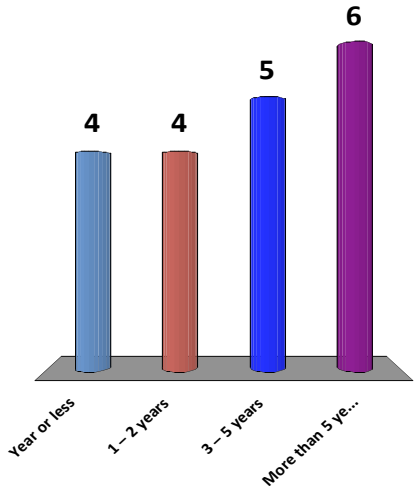
III. Results of The Focus Group

We present select highlights of the focus group in the discussion sections that follow.
The full results of the focus group are attached as Appendix 1: ICT SCRM Focus Group Polling Results, on page 24.

We started the focus group by asking respondents about themselves and their perspectives on the ICT SCRM industry. In regards to baseline characteristics of the focus group participants: eight of nineteen respondents have worked on ICT SCRM issues for two years or less; five respondents have worked on it for three to five years; and six respondents have worked on it for more than five years as shown below. There are few veterans in this space, given the relative newness of the ICT SCRM discipline.

How long have you personally been working on Supply Chain Risk Management issues?

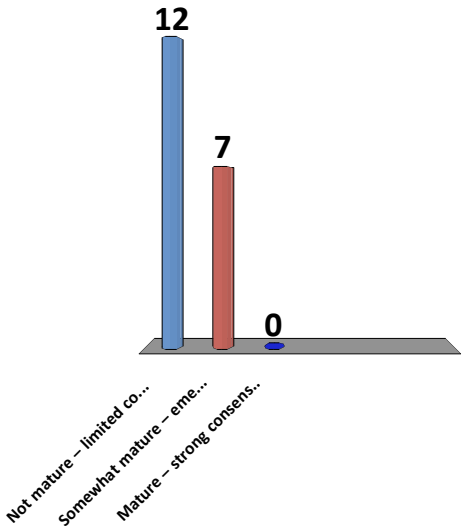
1. Year or less
2. 1 to 2 years
3. 3 to 5 years
4. More than 5 years



The newness of the discipline was a strong theme expressed by participants. When asked to rate the maturity of the ICT SCRM industry, twelve of nineteen respondents rated the industry as immature; and seven as somewhat mature. No one rated the industry as mature.

How would you rate the overall maturity of ICT SCRM industry practices and standards?

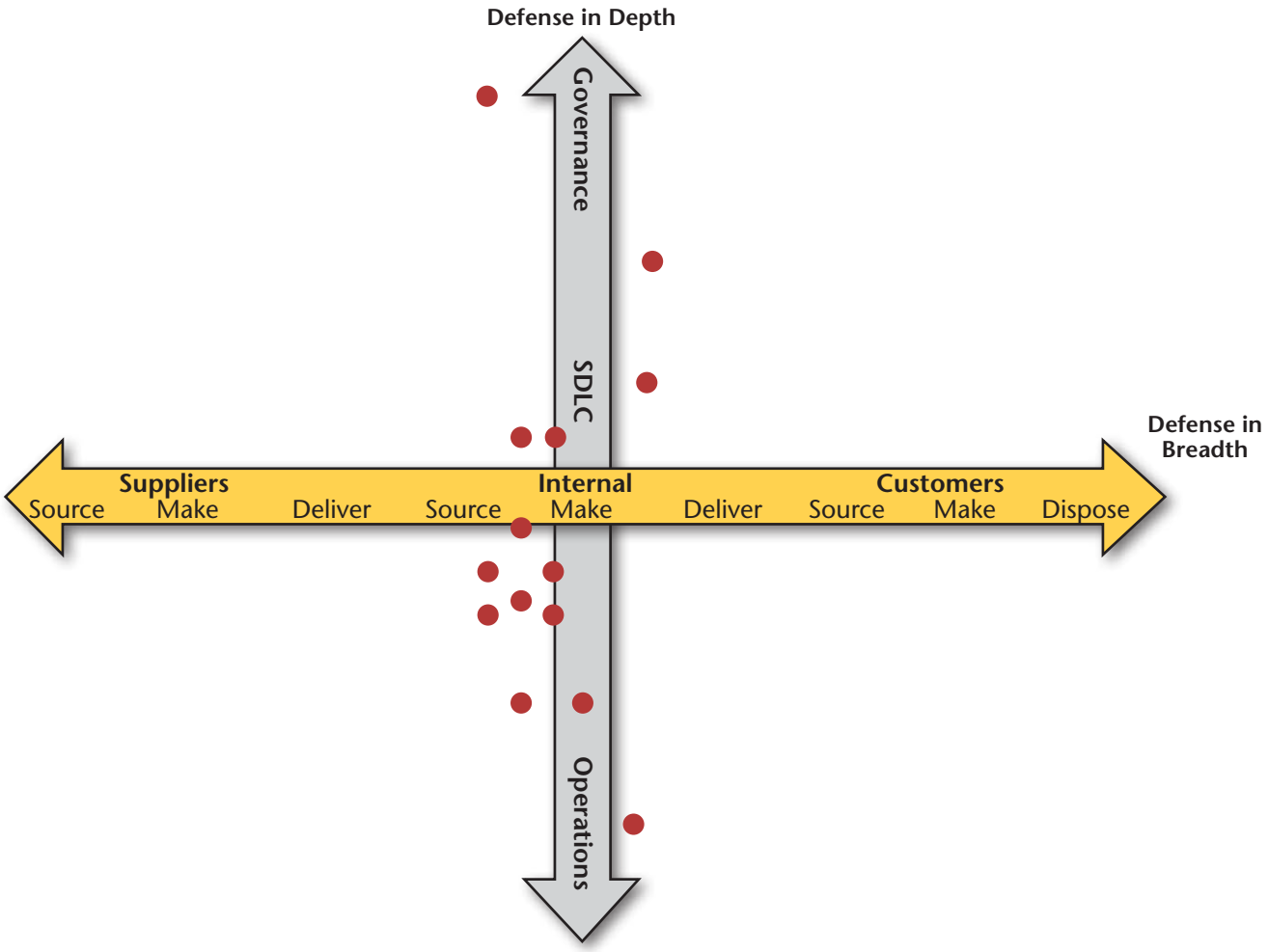
1. **Not mature** - limited consensus on effective practices and standards
2. **Somewhat mature** - emerging but incomplete consensus on effective practices and standards
3. **Mature** - strong consensus on effective practices and standards



The immaturity of the industry is a recurrent theme of our research for NIST. In our earlier work, "Toward a Cyber-Supply Chain Code of Practice" (March 2011), we examined some 200 ICT vendors of varying sizes through in-depth survey and concluded: "The cyber supply chain discipline is currently in an early emerging state characterized by: a deficient evidence-based body of knowledge; a proliferation and fragmentation of industry best practices and standards groups, generally led by the largest firms; and a profound under-usage of supply chain-wide risk governance mechanisms inside IT vendors" (p. 45).

This immaturity is reflected in the Strategic Positioning Graph *(see next page)* that we prepared based on our review of over sixty policy and practice documents of key initiatives in the marketplace and that we presented to the focus group for comment.

Strategic Positioning Graph: A Snapshot of the State of Community Initiatives



The graph above-while representing a rather static snapshot of an evolving ecosystem-nevertheless shows a clear clustering of current or proposed efforts around the internally-oriented systems development and supplier-oriented sourcing functions of defense in depth and breadth.

At the high end of the spectrum of activities along the defense in depth axis, there appear to be extensive gaps in coverage of Risk Governance.

In fact, enterprise risk management located at the most executive level of the organization is not addressed by most ICT SCRM organizations, initiatives and sets of industry practices. Further, there is a clear lack of an enterprise risk management function that spans the entire supply chain to coordinate adequate defense in breadth. This lack of coverage was first identified in our ICT SCRM Vendor Survey for NIST where we found that:

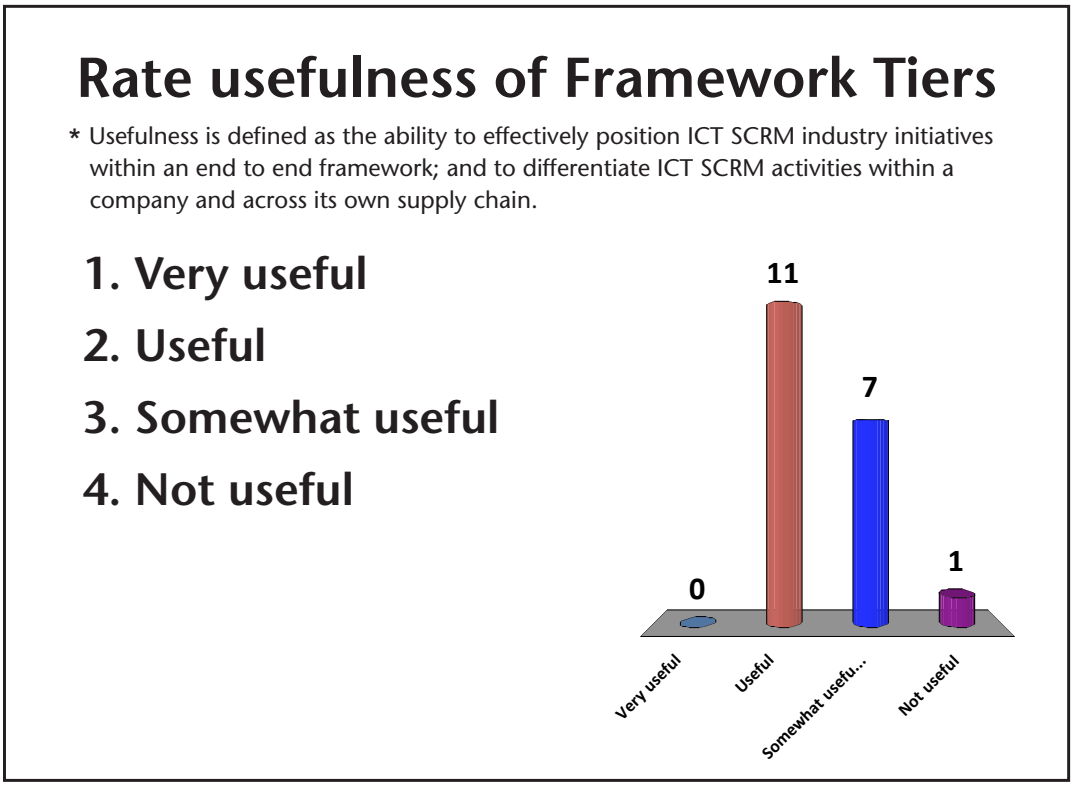
"On the strategic side of risk management, 47.6 percent of our sample of companies never uses a Risk Board or other executive mechanisms to govern risk; 46.1 percent never uses a shared Risk Registry, an online database of IT supply chain risks; 49.4 percent never uses an integrated IT supply chain risk management dashboard; and 44.9 percent say they never use a supply chain risk management plan" (ibid, p.20).

At the other end of the defense in depth axis, there are white spaces at the lowest level of field operations where ICT organizations seem to function without automated business rules and sensor-driven responses, e.g. they cannot sense and respond to risks in real time.

Participants generally agreed with the findings of the Strategic Positioning Graph above, while at the same seeking to express their own organizations' intentions to address these gaps; and calling for more sensitive and dynamic ways to measure emerging organizational capabilities.

Rating the Usefulness of Our Community Framework

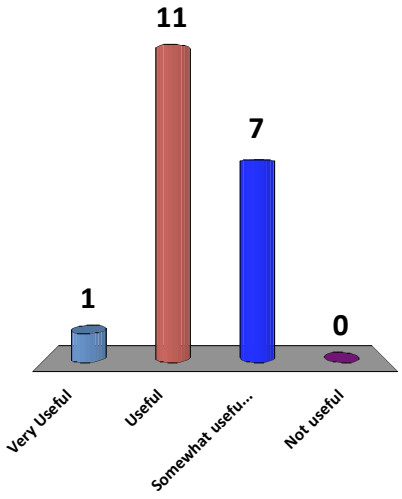
We then asked respondents to rate the usefulness of the Reference Framework Tiers and Attributes. Eleven of nineteen respondents rated the categorization of Tiers as useful; and seven rated it somewhat useful as shown below:



A very similar pattern of voting emerged in the rating of the Attributes, with Attributes mostly being voted as useful or somewhat useful by most of the respondents as shown below:

Define and Rate Tier 1 (Governance) Attributes

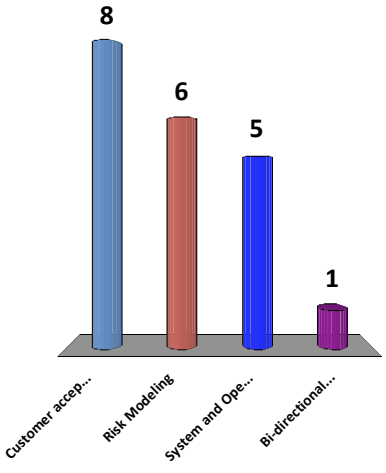
1. Very useful
2. Useful
3. Somewhat useful
4. Not useful



We asked the respondents to identify gaps in our list of Attributes and we then asked them to rank the gaps they collectively identified by criticality, as shown in the table below:

Which in your view is the most critical gap on the list?

1. Customer acceptance of risk mgt. responsibilities and obligations (contractual or otherwise)
2. Risk Modeling
3. System and Operational Risk controls
4. Bi-directional incident response (customer/supplier cooperation)



Customer acceptance of risk management responsibilities was the most critical gap. As we discovered in our previous survey for NIST, ICT vendors have a natural tendency to pay attention to and collaborate more with customers than suppliers in jointly monitoring supply chain risks. 42 percent of the sample collaborated in monitoring supply chain risks with their customers frequently and extensively versus 29 percent with suppliers. This focus group, however, seemed to express frustration with customers not taking responsibility for the supply chain risk management actions that must follow joint monitoring and discovery of incidents, exceptions and disruptions.

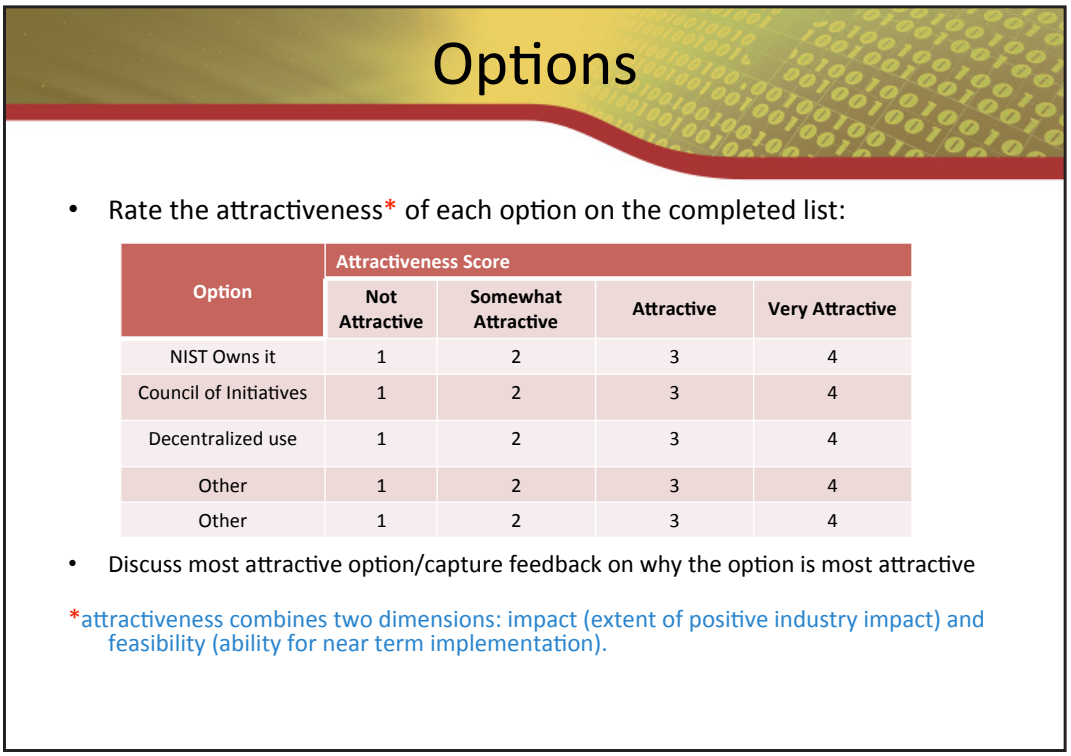
Having reviewed the Framework structure with participants, we then asked them to review how we coded the extent to which initiatives address or explicitly mention our Framework Tiers and Attributes. Based on their feedback, we have updated our coding and modified our Summary of Initiative Attributes, which compared each initiative along multiple dimensions, or attributes. Each initiative was assigned a simple three point rating score based on the extent to which it appeared to address a specific attribute. ***Please see Appendix 2: ICT SCRM Community Framework Tiers and Attributes, on page 58.***

Defining and Prioritizing Next Steps

Finally, we asked participants to define the attractiveness of future options to build out the Community Framework. By attractiveness, we combined two dimensions: industry impact and near term implementation feasibility. Our research team had defined a straw man set of options that included NIST owning the Community Framework; creating an external Council of Initiatives to help NIST develop it; or letting each organization use the Framework as it needed in a highly decentralized way.

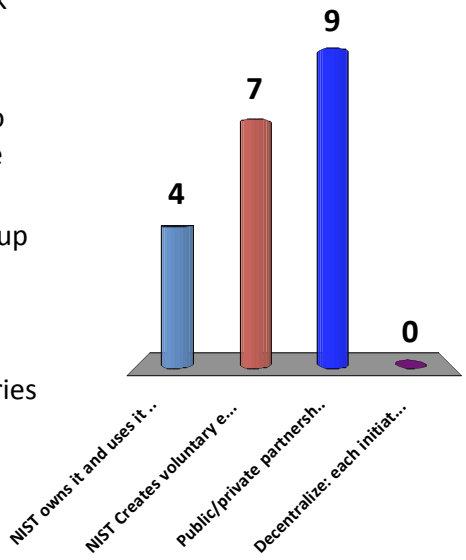
The focus group participants added the option of an independent public/ private partnership fully managing the Framework's development.

The preferred options were an independent public private partnership model to spur further community development which received nine votes of nineteen cast; and NIST creating a Council of Initiatives which received seven votes. Thus, 16 of 19 votes cast were for a collaborative government/industry model.



Attractiveness Score

- NIST owns it and uses it in own work to inform special publications
- NIST Creates voluntary external stakeholders Council of Initiatives to help facilitate information exchange
- Public/private partnership activity – eg. SCC hosts ICT SCRM interest group composed of the initiatives
- Decentralize: each initiative independently understands its own positioning in the framework and tries to cooperate with complimentary initiatives

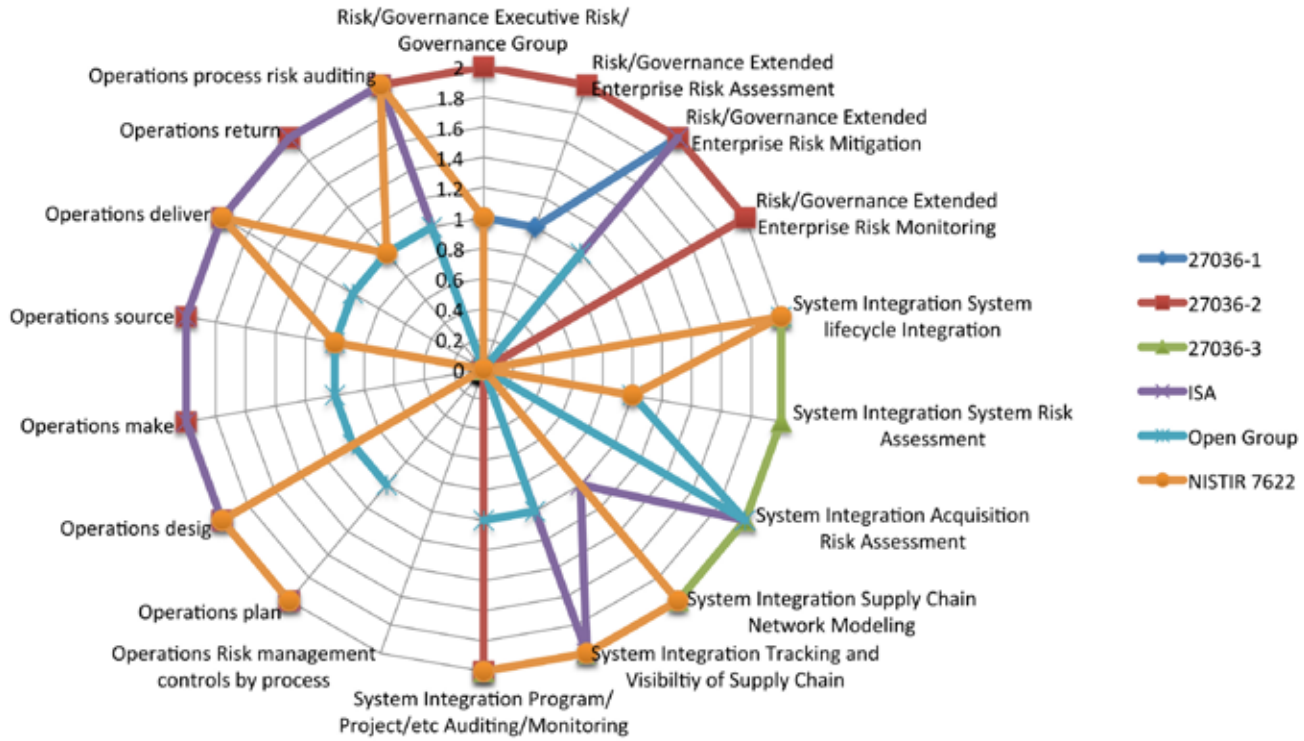


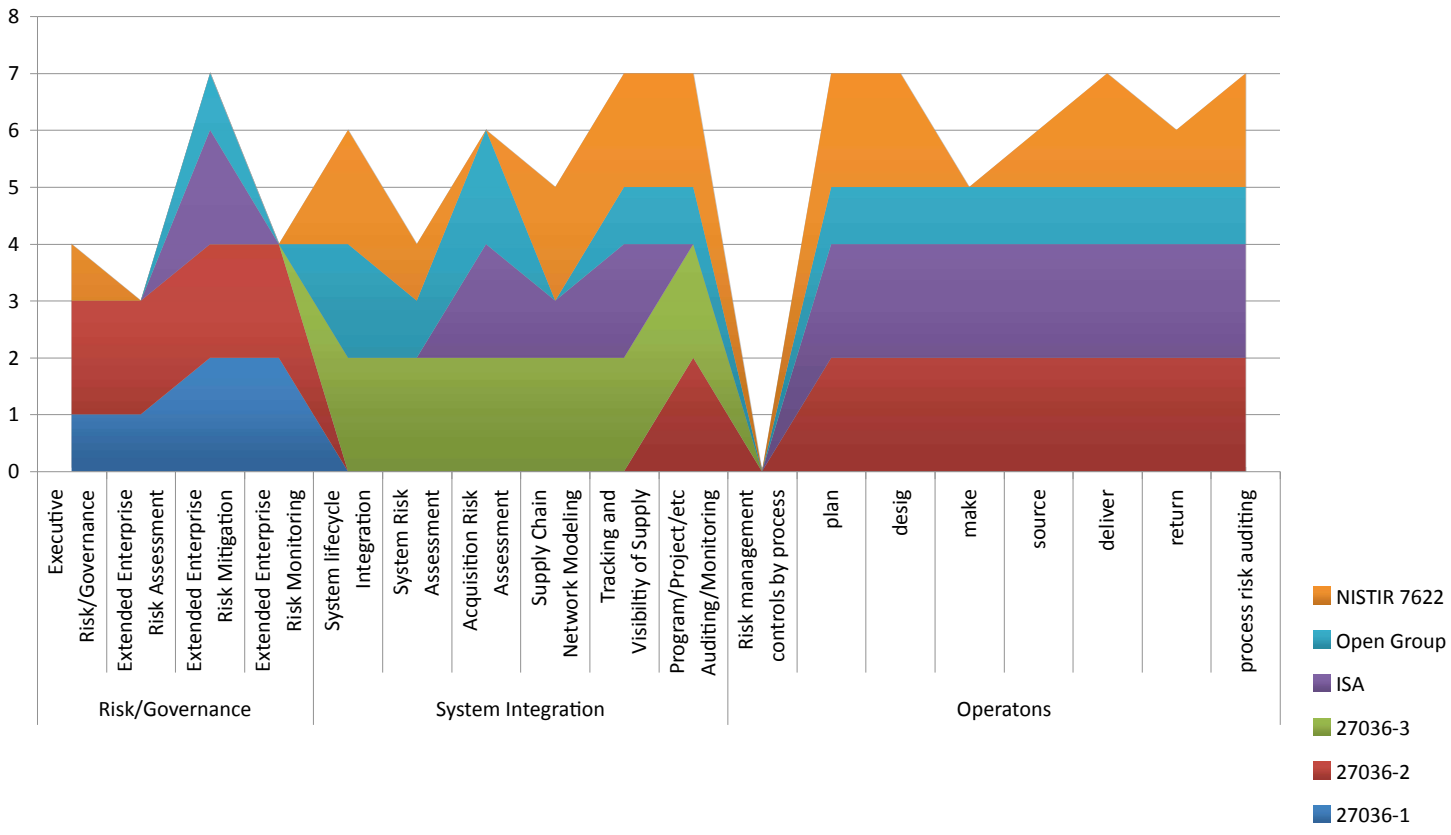
Post- Focus Group Revisions to the Community Framework

Participants were asked to return more detailed individual feedback on our preliminary Community Reference Framework architecture within a week of the focus group. We have attempted to embed that feedback into a major upgrade of our preliminary design. Our initial mapping approach of placing organizations as relatively static points on a graph of ICT SCRM focus areas (as represented in our Industry Positioning Graph) has been transformed into more kinetic Radar Graph displays that show an organization's span of coverage across key ICT SCRM Reference Framework Tiers and Attributes.

This moves the mapping of both uni-organizational and multi-organizational capabilities closer to more dynamic, total system lifecycle mapping approaches. These models address the call by participants for more "constructive layering" of diverse practice-sets and standards within an organization so as to better understand the spectrum of both it's current and emerging capabilities; and to show evolving synergies among key ecosystem actors.

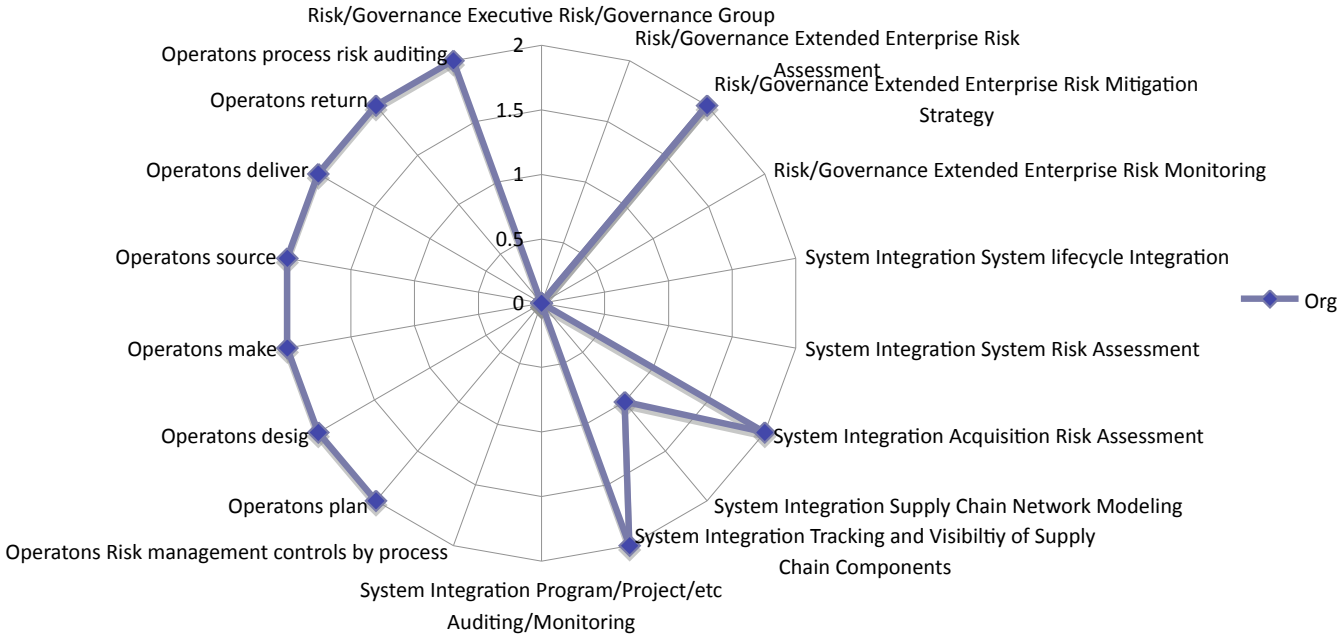
In the Radar Graphs below, we represent the overlapping spans of coverage of five key ICT SCRM initiatives (including the Open Group, ISA and the major three ISO ICT SCRM Standards Development Initiatives) we have examined in close detail:





We have also taken the suggestion to heart of seeking to present **an organizational self-mapping approach.** We have taken the revisions of a participating organization to its own ICT SCRM coverage information to show how it perceives itself in regards to its programmatic coverage of the Tiers and Attributes of our Framework, as shown below:

Organization A



Finally, we have updated the Detailed Matrix of Initiatives based on new information received from participants after we conducted the focus group. ***To view the updated Detailed Matrix of ICT SCRM Initiatives, please see Appendix 3, on page 65.***

IV. Conclusions/Recommendations

As the ICT SCRM Industry matures, we are slowly seeing a consensus emerge across initiatives.

The ICT SCRM Community Framework Project has added value by mapping the leading initiatives that seek to improve a common understanding of protecting the cyber supply chain. Each initiative has approached the problem from the viewpoint of their own constituents in an effort to articulate a way forward from a policy point of view or just to share content about practices.

Yet, our research shows from a detailed content point of view, that there are numerous examples where practices are consistent across organizations and initiatives which indicates that there is congruence about some of the protective practices both in the realm of defense in depth and defense in breadth, as shown below:

Emerging SCRM Consensus Areas Across Initiatives					
Attributes | Initiatives		Open Group	ISA	ISO 27036	NIST
Key Practices	Continous evaluation and optimization of practices	x		x	x
	Practices documented and standardized	x	x	x	x
	Vendor Performance measurement Scorecard	x		x	x
Process	Unified validation processes	x	x		x
	Threat Modeling	x	x		
	Risk Assessment	x		x	x
	Vulnerability Analysis & Response	x	x	x	x
	Product Development & Auditing Process				x
	Risk Mitigation Options		x	x	x
Technology	Defined secure coding standards	x		x	
	Physical Security Access Controls	x			x
	Automation & Documentation Assets	x			
	Categorization of Information Systems		x		x

For more details, please see the table in Appendix 4: Emerging ICT SCRM Consensus Areas, on page 93.

Going forward, there will certainly be value in continuing to examine these initiatives in terms of what they are targeting and when they could hope to realize their benefits. This will enable us to differentiate tactical from long term benefits as below:

- Tactical benefit: Content about Practices available for reading and using now
- Tactical benefit: Content about practices to be formalized in a standard within 18 months
- Tactical benefit: Method of verification available within a year- 18 months
- Long term benefit: Final Content about practices formalized in approved standard after 18 months from now
- Long term benefit: Method of verification not likely to be available until after 18 months
- Long term benefit: Verification across a wide array of initiatives can then be benchmarked for comparative effectiveness and suitability by market vertical.

By visually showing the initiatives against their intended benefits/ contributions over time, one can see how they compare. Some are just about content, some hope to be formal but are far out in time due to their nature. Assume for the moment that all of them were to accomplish what they intend and that there were no conflicts and full harmony, what will be available and when? How would one write a narrative that explains how all of these relate in benefit and timing? This insight could give NIST a sense as to what they want to leverage over time and where the public/private partnership should continue its efforts.

Examining these initiatives over time would also allow us to identify what persistent gaps against the UMD Community Reference Framework will still exist up and down the Defense in Depth axis and across the Defense in Breadth axis.

Anchoring ICT SCRM to the More Mature Supply Chain Industry Will Help Accelerate Consensus Building and Overall Development

Leveraging our own research and that of the Supply Chain Council's SCOR® Model helps to anchor ICT SCRM in an older, more established discipline. In the 1990s, the supply chain community came together in a Voluntary Interest Group to develop a consensus governance approach, a total systems lifecycle methodology, and a detailed set of process and sub-process practices and metrics. This Supply Chain Operations Reference Model is today used by over 800 organizations both, private and public, to understand and manage supply chains and is the most widely accepted framework for supply chain management. SCOR® started based on the same level of concern and interest on the part of global product supply chain managers as shown today by the ICT supply chain manager to gain a solid grip on complex processes and establish effective decision/operational controls.

Recently, the Supply Chain Council completed a two year project, led by an industry/government working group, to upgrade and formalize an Enterprise Risk Management module of SCOR®. SCOR 9.0 includes Risk Management processes, practices, and performance indicators; and SCOR 10.0 includes further risk management elements.

The SCOR® Risk Management Implementation Approach directly identifies some of the challenges of implementing a supply chain risk management program:

Organizational Support: Supply chain risk management needs cross-functional participation, agreement and cooperation in order to succeed. It cannot be done within a department without significantly limiting the impact on the business. This requires executive level commitment and active participation. Building this is a critical first step in the implementation process.

Rules and Strategies: Before risk management activities can start, a decision must be made as to the approach and the strategy. The main guidelines for managing risks and the rationale behind them must be developed, documented and communicated.

Roles, Responsibility: Clear roles and responsibility are critical for any process or program. In the case of supply risk management, even more so. Cross-functional, company wide responsibility and authority are critical for success. In addition, supply risk management adds new responsibilities to existing jobs. These must be clearly communicated, current skill levels of incumbents assessed and corrections made (training or replacement) as required.

The SCOR® Model takes a phased approach to successfully addressing these strategic enterprise risk management challenges:

The SCOR Model supports effective ICT SCRM through a five phase approach.

Phase	Name	Deliverable	Resolves
Initial	BUILD	• Organizational Support • Risk Management Program	Who is the sponsor?
I	DISCOVER	• Supply-Chain Definition • Supply-Chain Risk Priorities • Project Charter/Risk Program definition	What will the program cover?
II	ANALYZE	• Scorecard • Benchmark • Competitive Requirements • Customer service requirements	What is the risk tolerance of your supply chain?
III	ASSESS	• Geo Map • Thread Diagram • Risk assessment	Initial Analysis – where and how big are the risks?
IV	MITIGATE	• Mitigation plans • Level 3, Level 4 Processes • Best Practices Analysis	Final Analysis – how will risk be eliminated or mitigated?
V	IMPLEMENT	• Opportunity Analysis • Mitigation Definition • Deployment Organization • Monitoring and response programs	How to deploy mitigations?

Source: LMI/Supply Chain Council

1

Source: Supply Chain Council and Logistics Management Institute

The SCOR® Enterprise Risk Management Module directly defines a Risk Governance Methodology that can potentially "plug the gaps" in the profile of capabilities currently exhibited by the ICT SCRM Community and help accelerate its maturation.

There is an urgent need-expressed by our focus group participants- for NIST to help facilitate a Formal Community of Aligned Organizations, a public/private partnership to speed up the development of an ICT SCRM knowledge base and a set of effective practices.

The product supply chain globalized in the 1990s. Today, the ICT supply chain is sourcing and distributing code, hardware and components over many of the same communications networks and trade logistics lanes and is now rapidly off shoring.

The great challenge of the ICT Supply Chain industry today is to come together as a community; to reach across the hardware, software, network and physical distribution divides to gain greater strategic command and control; to better leverage the lessons learned from other supply chain disciplines; and to more effectively navigate the serious opportunities and risks associated with the rapid globalization of ICT systems.

In other words, we need to create a community that can coalesce around the common core challenges of survival and growth.

This needs to be our next step together.

Clearly, given its long term historical role in facilitating industry/government interactions around standards development, NIST has a unique role to play in creating such a community, in ensuring a fair and effective playing field for all community participants, and in turbo charging the ICT industry's drive toward greater maturity.

To support community development, NIST should consider these next steps:

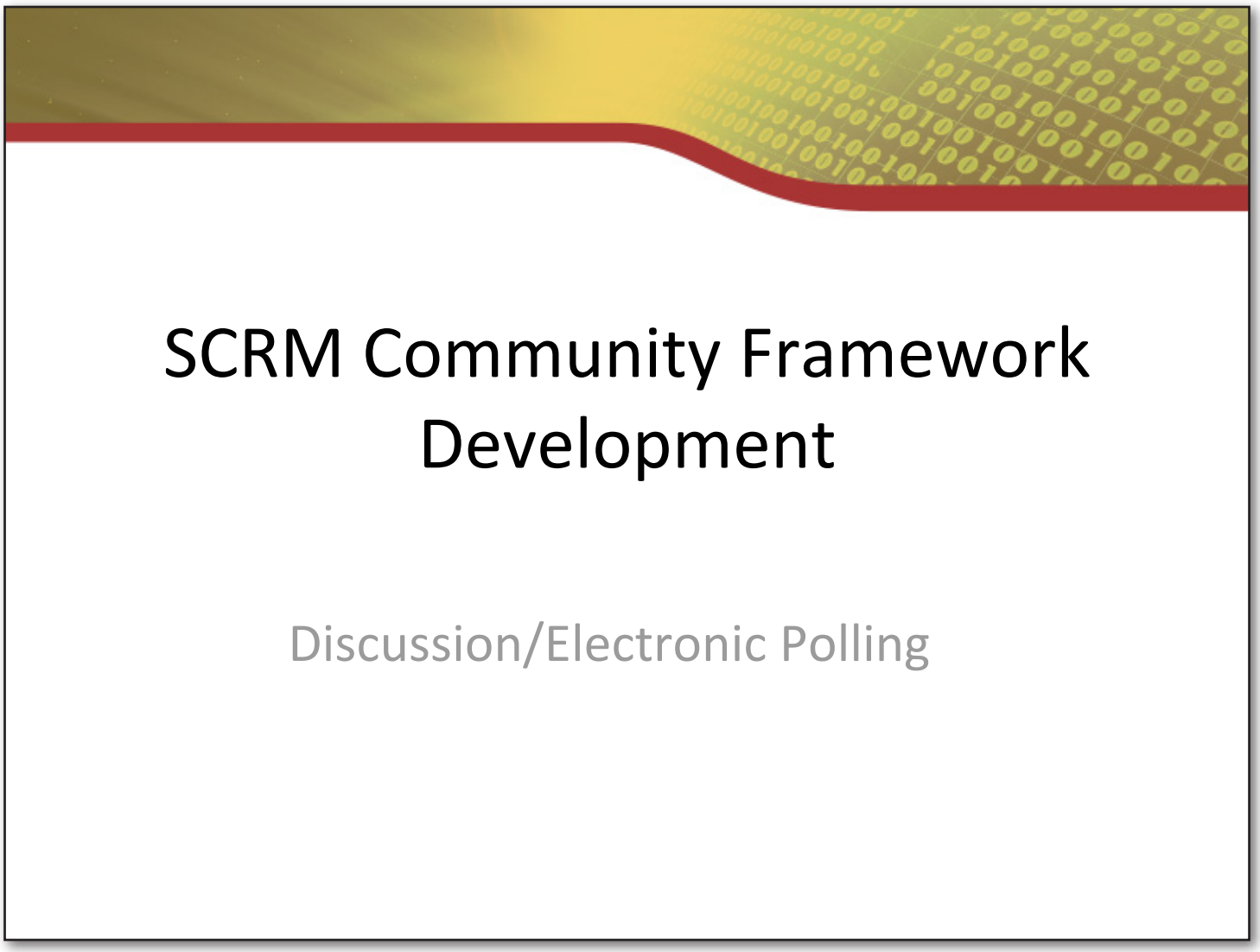
- Develop a charter and governance structure for a public/private consortium to address ICT SCRM.
- Provide facilitation and analytical support for the consortium.
- Perform a more detailed mapping of initiatives to clearly identify gaps in current and planned activities and recommend areas that NIST can address to create a more comprehensive ICT SCRM ecosystem.
- Perform a more detailed mapping to identify inconsistencies in ICT SCRM approaches that NIST can help reconcile.
- Develop a guidance document for using multiple frameworks/standards to develop a comprehensive ICT SCRM program.

- Develop a maturity model that specifically takes an organization from annual self-assessments into quarterly supply chain reviews progressing to monthly sense/detect sessions and eventually to continuous monitoring of defense in depth & defense in breadth.
- Develop a methodology and toolset to support self-assessment.
- Create a technical support group for assisting the cyber supply chain community to evaluate practices and standards.

To Conclude: Our core research finding is that a wide swathe of the ICT SCRM community believes NIST has a pivotal role to play in accelerating the growth and maturity of community practices and standards.

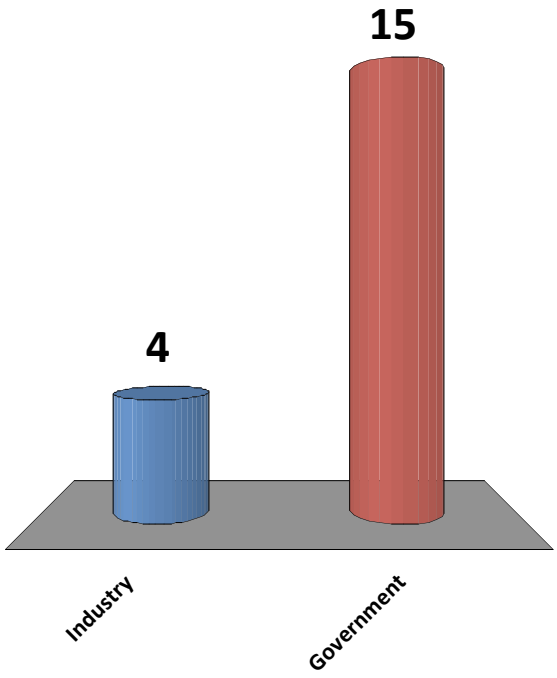
APPENDIX 1

ICT SCRM Focus Group Polling Results



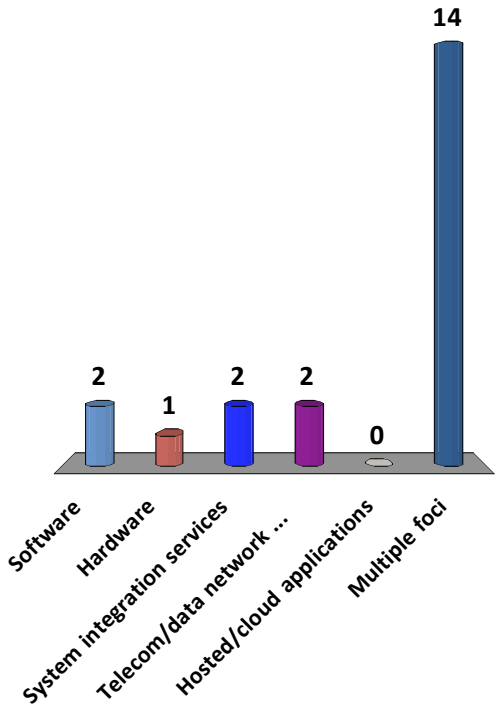
Which sector do you represent?

1. Industry
2. Government



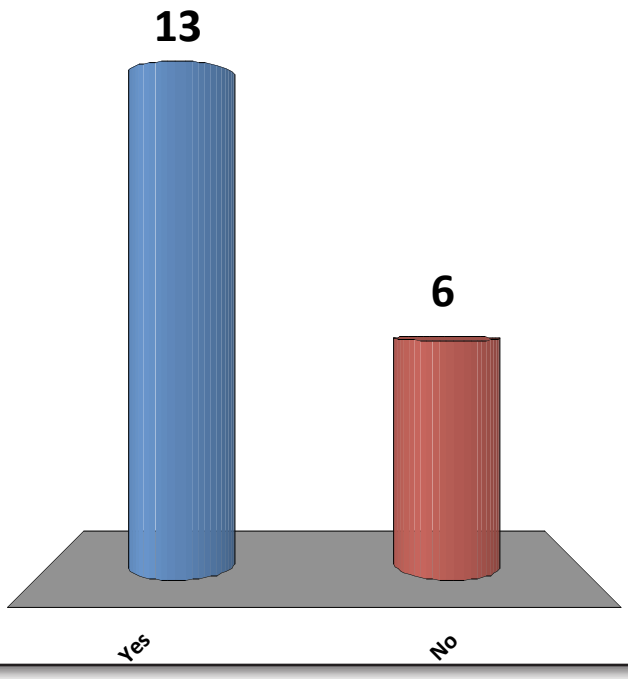
Is your home organization primarily focused on:

1. Software
2. Hardware
3. System integration services
4. Telecom/data network provisioning
5. Hosted/cloud applications
6. Multiple foci



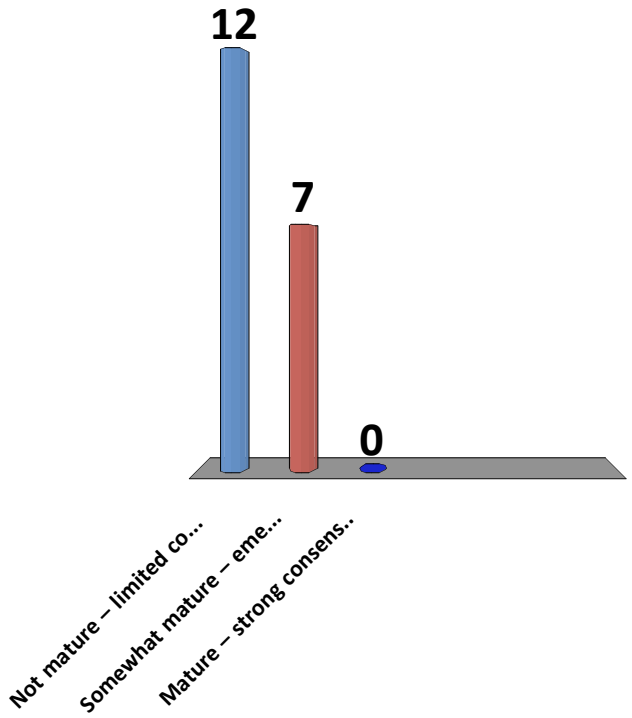
Do you represent a specific initiative covered by our framework?

1. Yes
2. No



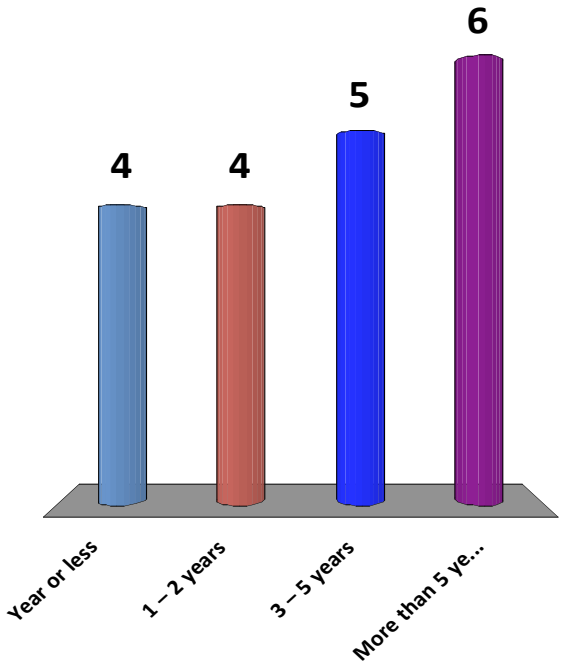
How would you rate the overall maturity of SCRM industry practices and standards?

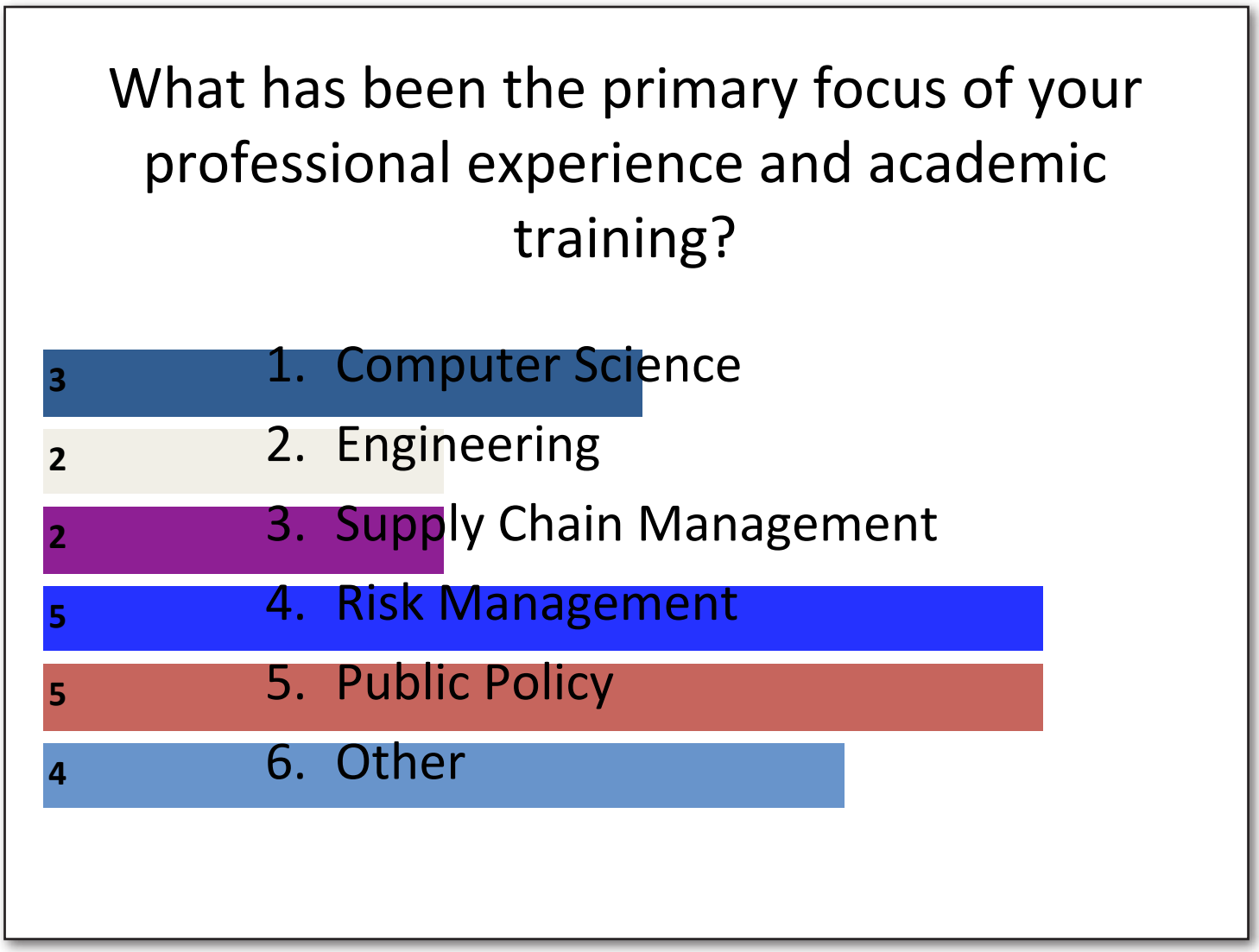
1. **Not mature** – limited consensus on effective practices and standards
2. **Somewhat mature** – emerging but incomplete consensus on effective practices and standards
3. **Mature** – strong consensus on effective practices and standards



How long have you personally been working on Supply Chain Risk Management issues?

1. Year or less
2. 1 – 2 years
3. 3 – 5 years
4. More than 5 years




What has been the primary focus of your professional experience and academic training?
3
1. Computer Science
2
2. Engineering
2
3. Supply Chain Management
5
4. Risk Management
5
5. Public Policy
4
6. Other

1. Framework

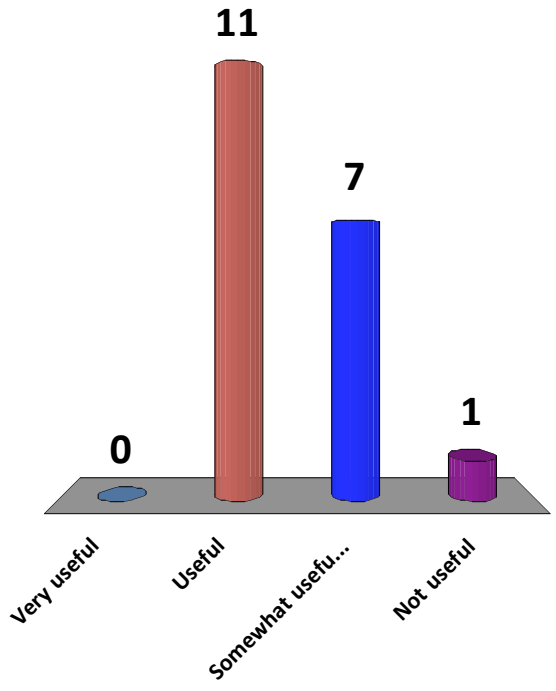
- Rate Usefulness* Of Framework Tiers-
  - very useful
  - useful
  - somewhat useful
  - not useful
- Discuss/Capture Missing Tiers

*usefulness is defined as ability to effectively position SCRM industry initiatives within an end to end framework; and to differentiate SCRM activities within a company and across its own supply chain.

Rate usefulness of Framework Tiers

*usefulness is defined as ability to effectively position SCRM industry initiatives within an end to end framework; and to differentiate SCRM activities within a company and across its own supply chain.

1. Very useful
2. Useful
3. Somewhat useful
4. Not useful



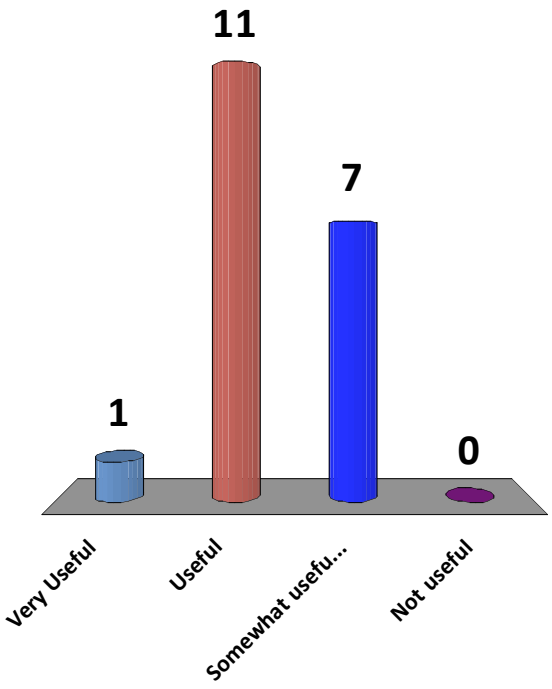
Framework

- Rate Usefulness Of Attributes In Each Tier:
- Define and rate Tier 1 (Governance)Attributes:
  - very useful
  - useful
  - somewhat useful
  - not useful

  - Discuss/Capture Tier 1 Missing Attributes

Define and rate Tier 1 (Governance)Attributes

1. Very Useful
2. Useful
3. Somewhat useful
4. Not useful



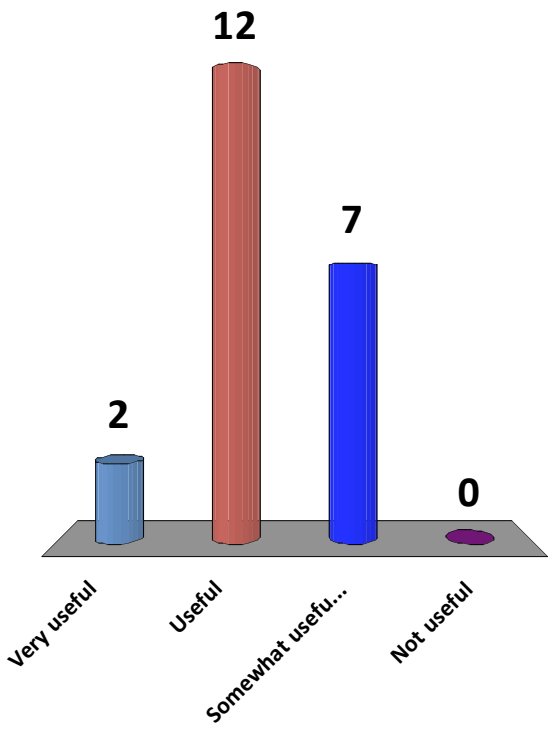
Framework

- Define and Rate Usefulness Of Tier 2 (Systems Integration) Attributes:
  - very useful
  - useful
  - somewhat useful
  - not useful

- Discuss/Capture Tier 2 Missing Attributes

Define and Rate Usefulness Of Tier 2 (Systems Integration) Attributes

1. Very useful
2. Useful
3. Somewhat useful
4. Not useful



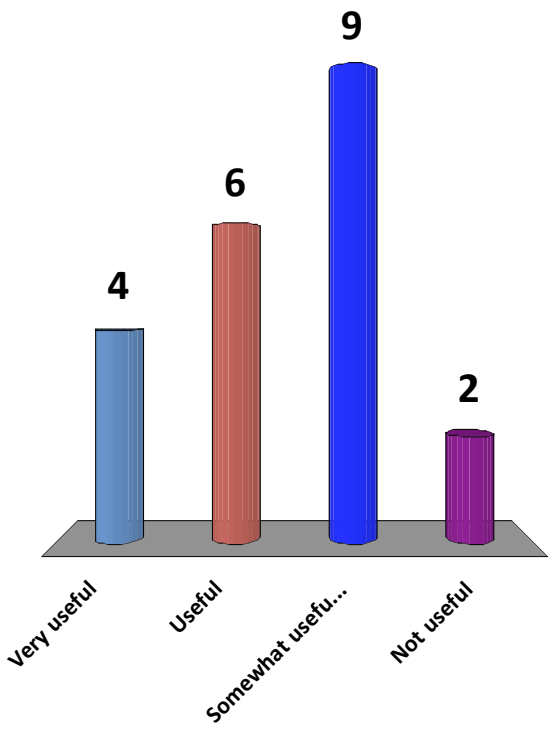
Framework

- Define and Rate Usefulness Of Tier 3 (Operations) Attributes:
  - very useful
  - useful
  - somewhat useful
  - not useful

- Discuss/Capture Tier 3 Missing Attributes

Define and Rate Usefulness Of Tier 3 (Operations) Attributes

1. Very useful
2. Useful
3. Somewhat useful
4. Not useful



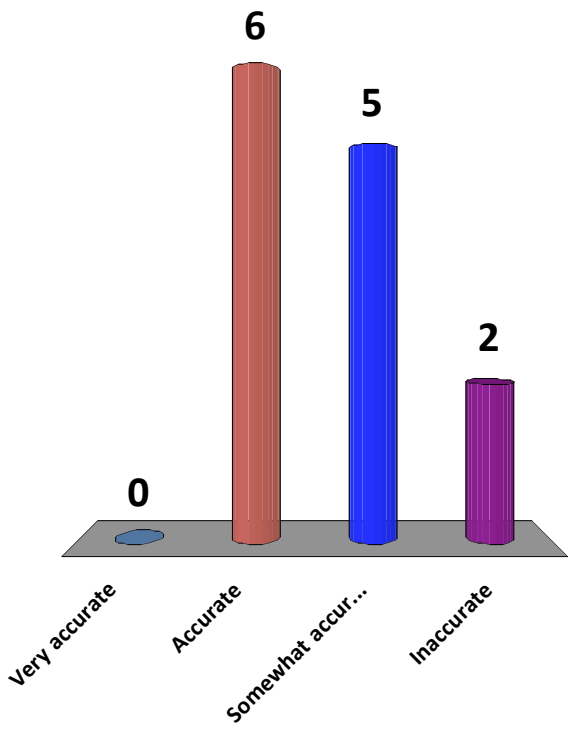
Framework

- Review our coding of the extent to which each initiative addresses the attributes within each tier (Harvey Balls)
- Rate the accuracy of our coding for your own initiative:
  - Very accurate
  - Accurate
  - Somewhat accurate
  - Inaccurate

- Discuss/capture sources of inaccuracies

Rate the accuracy of our coding for your own initiative:

1. Very accurate
2. Accurate
3. Somewhat accurate
4. Inaccurate



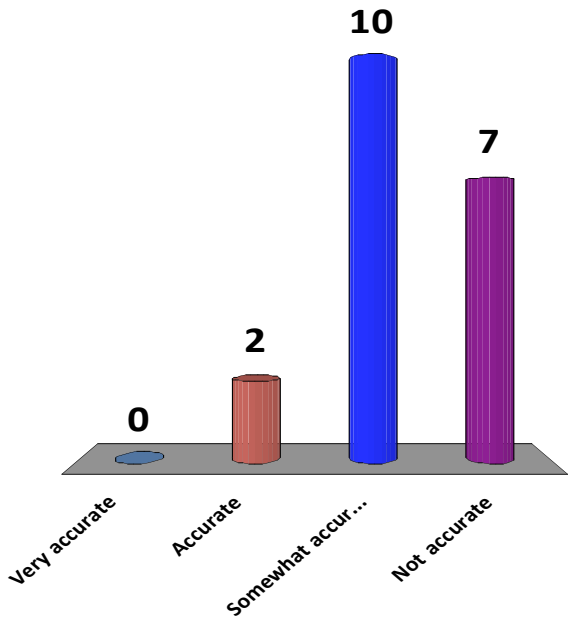
2. Characterization Of Initiatives

- Review our High Level Strategic Positioning Graph
- Based on your knowledge of the overall SCRM strategic landscape and the positioning of initiatives within it, how would you rate the accuracy of our graph:
  - Very accurate
  - Accurate
  - Somewhat accurate
  - Inaccurate

- Discuss/capture sources of inaccuracies

Based on your knowledge of the overall SCRM strategic landscape and the positioning of initiatives within it, how would you rate the accuracy of our graph:

1. Very accurate
2. Accurate
3. Somewhat accurate
4. Not accurate



Characterization Of Initiatives

- Use your knowledge of the SCRM industry landscape to re-position your own initiative and others on the hard copy of the Strategic Positioning Graph we have provided
- Review and Discuss Modifications to the Graph

3. Gap Analysis

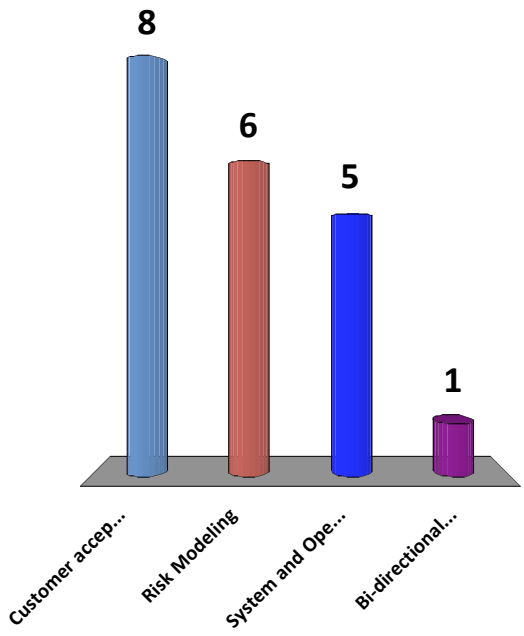
- Review both Strategic Positioning Graphs-our graph and the one you have just marked up
- Where do Initiatives cluster along the X/Y axis in both graphs? Do gaps exist in Initiative coverage of defense in depth and defense in breadth focus areas?
- List obvious gaps in coverage
- Discuss/capture other possible gaps

Gap Analysis

- Create a comprehensive list of gaps in coverage
- Rate the items on the list. Which, in your view, are the two most critical gaps on the list?
- Discuss/capture if any initiatives are working to fill those gaps in coverage in the near or midterm.

Which in your view is <u>the most</u> critical gap on the list?

1. Customer acceptance of risk mgt. responsibilities and obligations (contractual or otherwise)
2. Risk Modeling
3. System and Operational Risk controls
4. Bi-directional incident response (customer/supplier cooperation)



Please make your selection...

1. Choice One
2. Choice Two

Which three are the most important critical gaps – choose 3 in order of importance

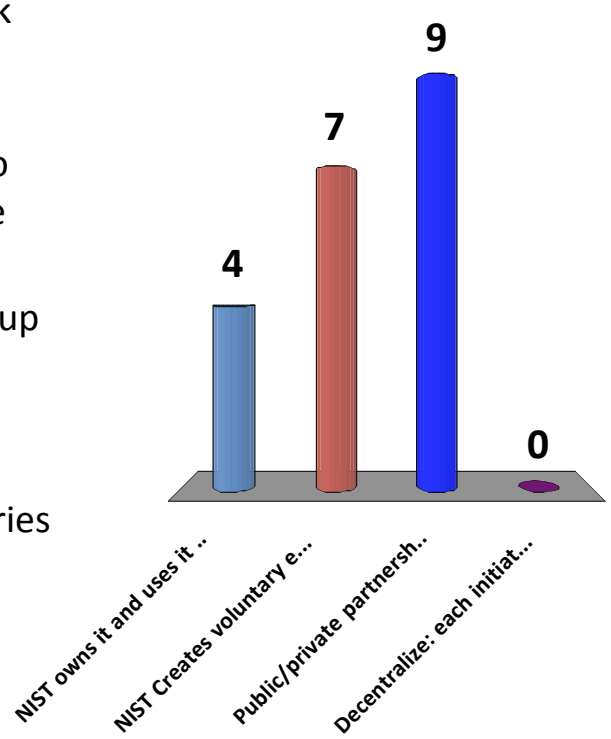
1. Gap 1 (fill this in as collected during discussion)
2. Gap 2
3. Gap 3
4. Gap 4
5. Gap 5

4.Options

- We have formulated some possible options for building out the Community SCRM Reference Architecture:
  - NIST owns it and uses it in own work to inform special publications
  - NIST Creates voluntary external stakeholders Council of Initiatives to help facilitate information exchange
  - Public/private partnership activity – eg. SCC hosts ICT SCRM interest group composed of the initiatives
  - Decentralize: each initiative independently understands its own positioning in the framework and tries to cooperate with complimentary initiatives.
- Discuss/capture what other options can be added to the list.

Attractiveness score

- NIST owns it and uses it in own work to inform special publications
- NIST Creates voluntary external stakeholders Council of Initiatives to help facilitate information exchange
- Public/private partnership activity – eg. SCC hosts ICT SCRM interest group composed of the initiatives
- Decentralize: each initiative independently understands its own positioning in the framework and tries to cooperate with complimentary initiatives



Options

- Rate the attractiveness* of each option on the completed list:

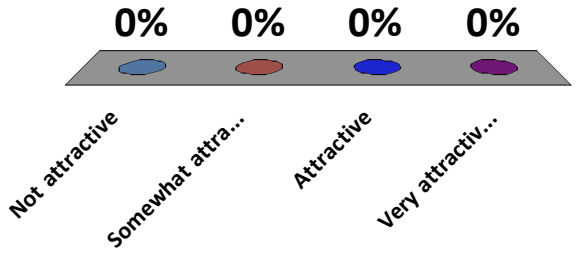
Option	Attractiveness Score			
	Not Attractive	Somewhat Attractive	Attractive	Very Attractive
NIST Owns it	1	2	3	4
Council of Initiatives	1	2	3	4
Decentralized use	1	2	3	4
Other	1	2	3	4
Other	1	2	3	4

- Discuss most attractive option/capture feedback on why the option is most attractive

*attractiveness combines two dimensions: impact (extent of positive industry impact) and feasibility (ability for near term implementation).

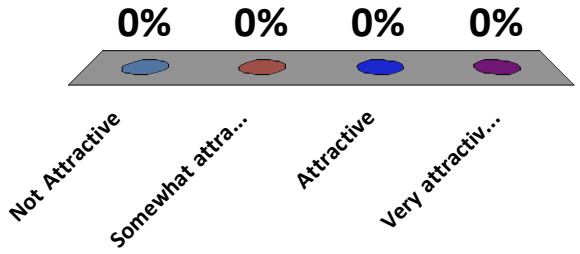
Attractiveness Score - Option A: NIST Owns it

1. Not attractive
2. Somewhat attractive
3. Attractive
4. Very attractive



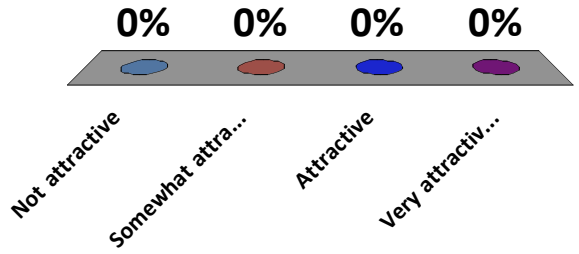
Attractiveness Score - Option B: Council of Initiatives

1. Not Attractive
2. Somewhat attractive
3. Attractive
4. Very attractive



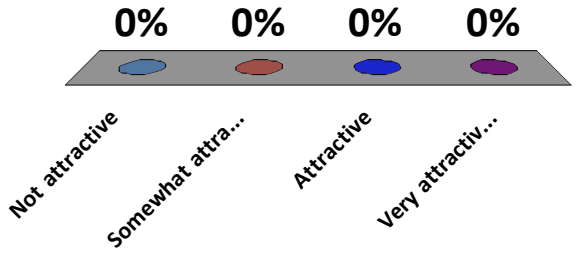
Attractiveness Score - Option C: Decentralized Use

1. Not attractive
2. Somewhat attractive
3. Attractive
4. Very attractive



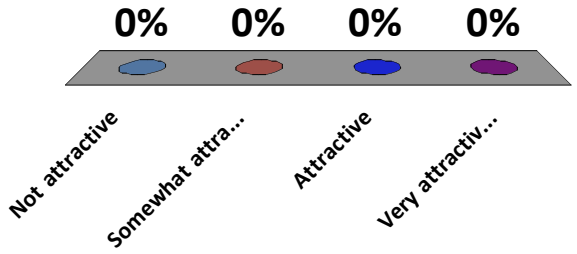
Attractiveness Score - Option D: Other

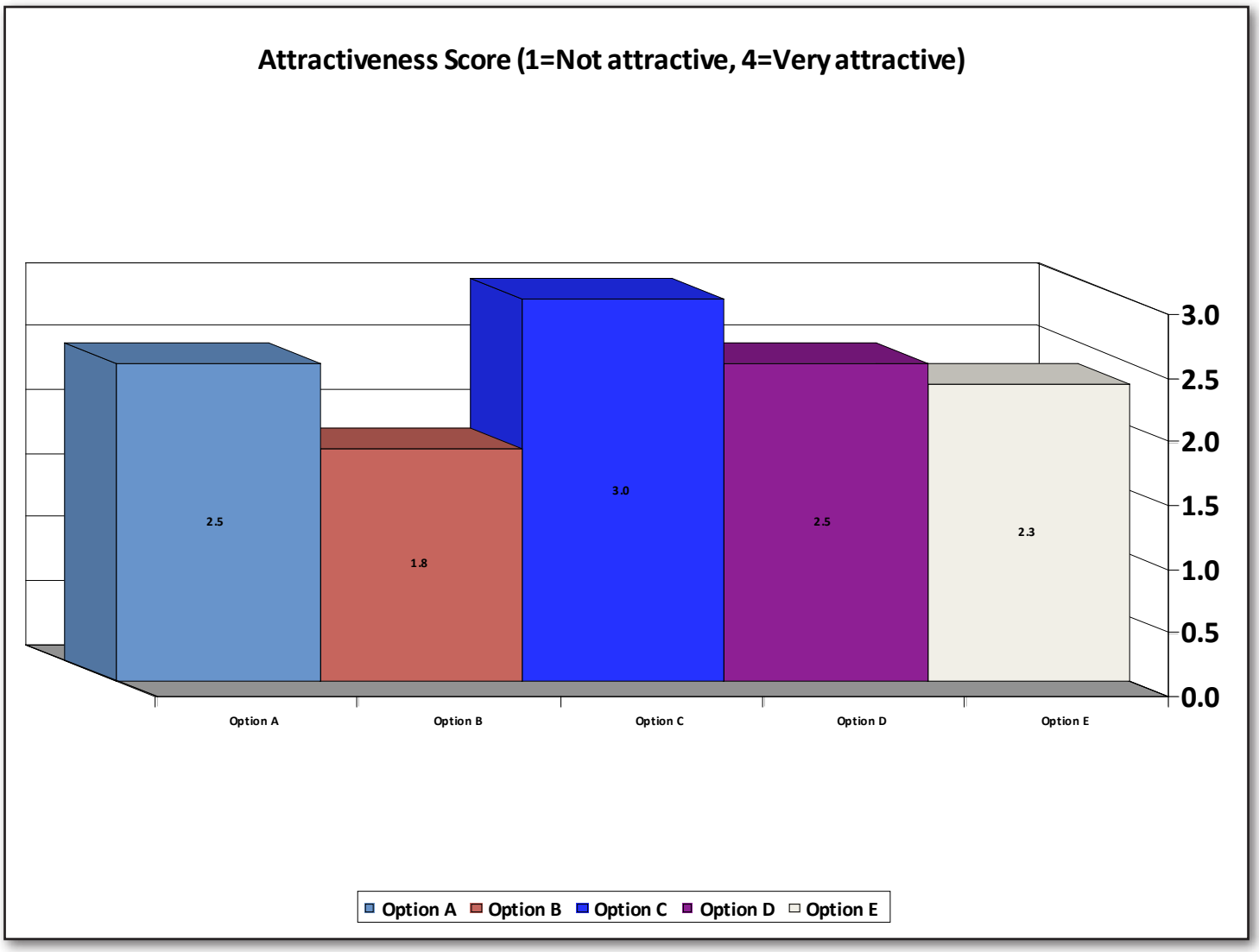
1. Not attractive
2. Somewhat attractive
3. Attractive
4. Very attractive



Attractiveness Score - Option E: Other

1. Not attractive
2. Somewhat attractive
3. Attractive
4. Very attractive




Attractiveness Score (1=Not attractive, 4=Very attractive)
2.5
1.8
3.0
2.5
2.3
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Option A
Option B
Option C
Option D
Option E
Option A
Option B
Option C
Option D
Option E

APPENDIX 2

ICT SCRM Community Framework Tiers and Attributes

LEGEND	
○	Not mentioned or mentioned infrequently, not discussed
◑	More frequently mentioned, cursorily discussed
●	Frequently mentioned, extensively discussed

Reference Framework Tier		Framework Attributes	SAFECODE		OPEN GROUP	ISA
			1	2	3	4
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	○	○	○	○
		Extended Enterprise Risk Assessment	○	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	◑	●
		Extended Enterprise Risk Monitoring	○	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	○	○	●	○
		System Risk Assessment/Threat Modeling	●	○	◑	○
		Acquisition Risk Assessment/Sourcing Management	○	●	●	●
		Supply Chain Network Modeling / Mapping	○	○	○	◑
		Tracking and Visibility of Supply Chain Components	○	○	◑	●
		Program/Project/Process Risk Auditing/Monitoring	○	○	◑	○
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:				
		Plan	○	○	◑	●
		Design	○	○	◑	●
		Make	●	●	◑	●
		Source	○	●	◑	●
		Deliver	○	●	◑	●
		Return	○	●	◑	●
		Process Risk Auditing	○	○	◑	●

ICT SCRM Community Framework Tiers and Attributes, cont.

Reference Framework Tier		Framework Attributes	CMU		
			5	6	7
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	○	○	○
		Extended Enterprise Risk Assessment	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	○
		Extended Enterprise Risk Monitoring	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	●	○	○
		System Risk Assessment/Threat Modeling	●	◑	◑
		Acquisition Risk Assessment/Sourcing Management	●	●	○
		Supply Chain Network Modeling / Mapping	○	○	○
		Tracking and Visibility of Supply Chain Components	○	○	○
		Program/Project/Process Risk Auditing/Monitoring	○	○	○
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:			
		Plan	○	○	○
		Design	○	○	○
		Make	○	○	○
		Source	○	○	○
		Deliver	◑	○	○
		Return	○	○	○
		Process Risk Auditing	○	○	○

Reference Framework Tier		Framework Attributes	NIST		
			8	9	10
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	◑	○	○
		Extended Enterprise Risk Assessment	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	○
		Extended Enterprise Risk Monitoring	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	●	●	●
		System Risk Assessment/Threat Modeling	◑	●	○
		Acquisition Risk Assessment/Sourcing Management	○	○	○
		Supply Chain Network Modeling / Mapping	●	○	○
		Tracking and Visibility of Supply Chain Components	●	○	○
		Program/Project/Process Risk Auditing/Monitoring	●	○	○
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:			
		Plan	●	○	○
		Design	●	○	○
		Make	○	○	○
		Source	◑	○	○
		Deliver	●	○	○
		Return	◑	○	○
		Process Risk Auditing	●	○	○

ICT SCRM Community Framework Tiers and Attributes, cont.

Reference Framework Tier		Framework Attributes	NIST		MICROSOFT	
			11	12	13	14
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	○	○	○	○
		Extended Enterprise Risk Assessment	○	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	○	○
		Extended Enterprise Risk Monitoring	○	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	○	●	●	●
		System Risk Assessment/Threat Modeling	○	○	○	○
		Acquisition Risk Assessment/Sourcing Management	●	○	◑	●
		Supply Chain Network Modeling / Mapping	○	○	○	○
		Tracking and Visibility of Supply Chain Components	○	○	○	○
		Program/Project/Process Risk Auditing/Monitoring	○	○	○	○
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:				
		Plan	○	○	○	○
		Design	○	○	○	○
		Make	○	○	○	○
		Source	○	○	○	○
		Deliver	○	○	○	○
		Return	○	○	○	○
		Process Risk Auditing	○	○	○	○

Reference Framework Tier		Framework Attributes	TELECOMM CARRIER WORKING GROUP	GISC	DOD
			15	16	17
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	●	○	○
		Extended Enterprise Risk Assessment	◑	○	◑
		Extended Enterprise Risk Mitigation Strategy	◑	○	●
		Extended Enterprise Risk Monitoring	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	○	○	●
		System Risk Assessment/Threat Modeling	○	○	○
		Acquisition Risk Assessment/Sourcing Management	○	○	●
		Supply Chain Network Modeling / Mapping	○	○	○
		Tracking and Visibility of Supply Chain Components	○	○	○
		Program/Project/Process Risk Auditing/Monitoring	○	○	●
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:			
		Plan	○	◑	○
		Design	○	○	○
		Make	○	◑	○
		Source	○	◑	○
		Deliver	○	◑	●
		Return	○	○	◑
		Process Risk Auditing	○	○	○

ICT SCRM Community Framework Tiers and Attributes, cont.

Reference Framework Tier		Framework Attributes	Common Criteria (NIAP etc.)			
			18	19	20	21
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	○	○	○	○
		Extended Enterprise Risk Assessment	○	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	○	○
		Extended Enterprise Risk Monitoring	○	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	○	○	○	○
		System Risk Assessment/Threat Modeling	◑	◑	◑	◑
		Acquisition Risk Assessment/Sourcing Management	○	○	○	○
		Supply Chain Network Modeling / Mapping	○	○	○	○
		Tracking and Visibility of Supply Chain Components	○	○	○	○
		Program/Project/Process Risk Auditing/Monitoring	○	○	○	○
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:				
		Plan	○	○	○	○
		Design	○	○	○	○
		Make	○	○	○	○
		Source	○	○	○	○
		Deliver	○	○	○	○
		Return	○	○	○	○
		Process Risk Auditing	○	○	○	○

Reference Framework Tier		Framework Attributes	DEPARTMENT OF HOMELAND SECURITY			
			22	23	24	25
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	○	○	○	○
		Extended Enterprise Risk Assessment	○	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	○	○
		Extended Enterprise Risk Monitoring	○	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	●	○	○	○
		System Risk Assessment/Threat Modeling	●	●	○	○
		Acquisition Risk Assessment/Sourcing Management	○	○	○	○
		Supply Chain Network Modeling / Mapping	○	○	○	○
		Tracking and Visibility of Supply Chain Components	○	○	○	○
		Program/Project/Process Risk Auditing/Monitoring	○	○	◑	○
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:				
		Plan	○	○	○	●
		Design	●	○	○	●
		Make	◑	○	○	●
		Source	○	○	○	○
		Deliver	○	○	○	○
		Return	○	○	○	○
		Process Risk Auditing	○	○	○	○

ICT SCRM Community Framework Tiers and Attributes, cont.

Reference Framework Tier		Framework Attributes	DEPARTMENT OF HOMELAND SECURITY			
			26	27	28	29
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	○	○	○	○
		Extended Enterprise Risk Assessment	○	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	○	○
		Extended Enterprise Risk Monitoring	○	○	○	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	○	○	○	●
		System Risk Assessment/Threat Modeling	●	○	○	○
		Acquisition Risk Assessment/Sourcing Management	○	○	○	○
		Supply Chain Network Modeling / Mapping	○	○	○	○
		Tracking and Visibility of Supply Chain Components	○	○	○	○
		Program/Project/Process Risk Auditing/Monitoring	○	○	○	○
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:				
		Plan	○	●	○	○
		Design	○	●	○	○
		Make	○	●	○	○
		Source	○	○	○	○
		Deliver	○	○	○	○
		Return	○	○	○	○
		Process Risk Auditing	○	○	●	○

Reference Framework Tier		Framework Attributes	INTERNATIONAL STANDARDS ORGANIZATION (ISO)		
			30	31	32
TIER I	**RISK GOVERNANCE:** (UMD / SCOR)	Executive Risk Governance Group	◑	●	○
		Extended Enterprise Risk Assessment	◑	●	○
		Extended Enterprise Risk Mitigation Strategy	●	●	○
		Extended Enterprise Risk Monitoring	●	●	○
TIER II	**SYSTEM INTEGRATION:** (UMD / SCOR)	System Lifecycle Integration / Design for Risk	○	○	●
		System Risk Assessment/Threat Modeling	○	○	●
		Acquisition Risk Assessment/Sourcing Management	○	○	●
		Supply Chain Network Modeling / Mapping	○	○	●
		Tracking and Visibility of Supply Chain Components	○	○	●
		Program/Project/Process Risk Auditing/Monitoring	○	●	●
TIER III	**OPERATIONS:** (SCOR / UMD)	Risk Management Controls, By Process:			
		Plan	○	●	○
		Design	○	●	○
		Make	○	●	○
		Source	○	●	○
		Deliver	○	●	○
		Return	○	●	○
		Process Risk Auditing	○	●	○

Framework Source Documents

FRAMEWORK SOURCE DOCUMENTS	
UMD	• Building a Cyber Supply Chain Assurance Reference Model • Towards a Cyber Supply Chain Code of Practice
SCOR	• Supply Chain Operations Reference (SCOR) Model • SCOR for IT • Managing the Risk in your Organization with the SCOR Methodology
NIST	• NIST - System Development Lifecycle 2008

LEGEND	
SAFECODE	Software Assurance Forum for excellence in code
CMU	Carnegie Mellon University
NIST	National Institute of Standards and Technology
ISA	Internet Security Alliance
DHS	Department of Homeland Security
DOD	Department of Defense

S. No	Document Name	Author	Category	Sub-Category
1	Fundamental Practices for Secure Software Development 2nd Edition	SAFECode	Best Practices	Software
2	Software Integrity Controls	SAFECode	Best Practices	Software
3	Open Trusted Technology Provider Framework (O-TTPF)	The Open Group	Best Practices	Software/Hardware
4	The ISA Guidelines for Securing the Electronics Supply Chain (Draft Version 6)	ISA	Best Practices	Hardware
5	Software Supply Chain Risk Management: From Products to Systems of Systems	CMU	Best Practices	Software
6	Evaluating and Mitigating Software Supply Chain Security Risks	CMU	Best Practices	Software
7	A Taxonomy of Operational Cyber Security Risks	CMU	Best Practices	IT Systems
8	NIST IR 7622 (draft) Notional Supply Chain Risk Management for Federal Information Systems	NIST	Best Practices	IT Systems
9	Risk Management Guide for Information Technology Systems	NIST	Best Practices	IT Systems
10	Contingency Planning Guide for Information Technology Systems	NIST	Best Practices	IT Systems
11	Guide to Selecting Information Technology Security Products	NIST	Best Practices	IT Systems
12	Recommended Security Controls for Federal Information Systems	NIST	Best Practices	IT Systems
13	Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust	Microsoft	Best Practices	Software
14	Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity	Microsoft	Best Practices	IT Systems

Framework Source Documents, cont.

S. No	Document Name	Author	Category	Sub-Category
15	Foreign Supply Chain Security Risk Management: A Proposed Model, Protecting the U.S. Public Telecommunications Network Infrastructure	Telecom Carrier Working Group	Process Framework/ Structured Methodologies	Telecomm Networks
16	US Reliance on Foreign IT, Mitigating Risks Associated with Foreign Sources of Hardware Components	Global Innovation and Strategy Center	Policy Reform	Hardware
17	Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program	DOD	Best Practices	Software
18	CC - Community NIAP Vision 11-10	NIAP	Policy Reform	IT Systems
19	Customers Perceptions about the Relevancy of Common Criteria for Supply Chain Security	NIAP	Policy Reform	Software
20	A CC Community for Supply Chain	NIAP	Policy Reform	Software/Hardware
21	Common Criteria, Embrace Reform Extend	Intel and Cisco	Policy Reform	Software/Hardware
22	Architecture and Design Considerations for Secure Software	DHS	Best Practices	Software
23	Software Assurance in Acquisition and Contract Language	DHS	Best Practices	Software
24	Software Supply Chain Risk Management and Due-Diligence	DHS	Best Practices	Software
25	Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses	DHS	Best Practices	Software
26	Requirements and Analysis for Secure Software	DHS	Best Practices	Software
27	Secure Coding	DHS	Best Practices	Software
28	Software Security Testing	DHS	Best Practices	Software
29	Software Assurance in Education, Training and Certification	DHS	Best Practices	Software
30	ISO/IEC JTC 1/SC 27 - N10131 - 270361 - N9965	ISO	Best Practices	IT Services
31	ISO/IEC JTC 1/SC 27 - N10XXX - 270362 - N9967	ISO	Best Practices	IT Services
32	ISO/IEC JTC 1/SC 27 - N10133 - 270363 - N9969	ISO	Best Practices	IT Services

APPENDIX 3

Detailed Matrix of ICT SCRM Initiatives

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
The Open Group	Open Trusted Technology Provider Framework (O-TTPF)	Best Practices	Software Hardware	Software/ Hardware developers	Enterprise Risk Mitigation Strategy	**Industry Best Practice:** The organization's supply chain management is aware of and actively participates in the evolution and optimization of industry practices and methods.
					System Lifecycle Integration/ Design for Risk	**Industry Best Practice:** Trusted technology providers utilize and internalize the application of a well-formed and documented development (or manufacturing) method or process.
						Industry Best Practice: Product engineering methods are specified and refined to best fit the engineering/development characteristics of the target product.
						Formal Product Engineering or Development Community: Product lifecycle practices and processes are supported by a community of practitioners who vigilantly maintain the organization's engineering practices.
						Secure Coding Standards: Trusted technology provides establish secure coding standards to avoid the most common coding errors that lead to exploitable product vulnerabilities.
						Industry Best Practice: Supply chain security and integrity is treated as a key element of the end-to-end development/ manufacturing process.
						Industry Best Practice: Validation technology and/or processes are embedded into the trusted supply chain.
						Physical Security: Physical security access controls are necessary to protect development assets, manufacturing process, the plant floor, and the supply chain.
						Access Controls Proper access controls are established for supply chain systems—intellectual property, inventory, customer fulfilment, shipping, etc. For example, a unique identity is recorded when changes are made to development/manufacturing assets.
						Personnel and Contractor Security: Background checks are conducted for all new personnel, employees, and contractors whose activities are directly related to product supply chains (within reason and according to local law). Periodic checks/audits of contractors are conducted. Supplier maintains a code of conduct applicable to its entire supply chain.
						Physical Security Training and Threat Awareness: Security personnel are trained to protect physical company assets and supply routes and are aware of potential and evolving threats.
						Information System Security: Suppliers ensure protection of customer Personally Identifiable Information (PII), confidential data, and development assets through an appropriate and complementary set of information system security controls.

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Secure Transmission and Handling: Development assets are transmitted and handled securely between trusted providers and their suppliers. A risk management approach is applied to prevent subversion and preserve the goodness of the product from inception through deployment (production).
					System Risk Assessment/ Threat Modeling	**Threat Modeling:** Threat modeling is a technique which identifies a set of potential attacks on a particular product or system and describes how those attacks might be perpetrated and the best methods of preventing potential attacks. Threat models are used as input to the creation of test plans and cases.
						Risk Assessment: Supply chain risk management is the identification, assessment, and prioritization of business, technical, and physical risks as it pertains to the use of third-party components and services during manufacturing and the delivery of the product to the end user. This is followed by a plan to mitigate risks against high priority assets.
						Risk Assessment: Multi-tiered accreditation program • Tier A: Self-Assertion and third-party administration • Tier B: third-party accreditation • Tier C: third-party accreditation of specific product compliance • Re-accreditation
					Acquisition Risk Assessment/ Sourcing Management	**Industry Best Practice:** Trusted technology providers select suppliers who follow equivalent secure development/ engineering practices for supplied components and follow hardening practices to secure their configuration.
						Industry Best Practice: A trusted technology provider manages suppliers through a framework that measures supplier performance against metrics such as quality, efficiency, innovation, adherence to the vendor's specifications, social responsibility, and their ability to manage their workforce and their internal supply chain.
						Industry Best Practice: Trusted technology providers require their suppliers to follow similar secure development/ engineering practices for supplied components.
						Industry Best Practice: Trusted technology providers employ a structured approach to inclusion of open source as components in their offerings.
						Business Partner Security: Business partners are screened to ensure they are not on exclusion lists and periodic audits are conducted to ensure adherence to supply chain and integrity guidelines.
						Trusted Components: Trusted technology providers require their suppliers to follow similar secure development/ engineering practices for supplied components and such practices are contractually required for high-assurance/high-risk components. This includes vulnerability response programs and configuration profiles.

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Industry Best Practice: The organization's product evaluation method follows internationally accepted industry and government best practices.
						Industry Best Practice: A trusted technology provider manages its product evaluations appropriate to customer requirements at defined assurance levels, providing products and supporting documentation to certified third-party laboratories as required.
						Industry Best Practice: Product evaluations are performed as part of product assurance.
						Cross-organizational support: Supplier has developed mature cross-organizational support for product-level certifications and accreditations. A formal centralized support function is necessary to provide expertise, promote asset re-use, promote funding, and resolve pervasive issues.
						Product evaluations are resourced as part of the development process: Product evaluations deemed necessary for business purposes are planned, resourced, and executed as part of the development process and in a timely manner.
						Automation and Documentation Assets: Supplier develops re-usable assets that reduce the amount of resources necessary to complete an evaluation or certification. Re-usable assets also increase accuracy of the evaluation process.
					Tracking and Visibility of Supply Chain Components	**Formal Product Acceptance:** Product engineering or development releases or changes require formal approval from product management.
					Program/ Project/Process Risk Auditing/ Monitoring	**Vulnerability Analysis and Response:** Vulnerability analysis is the process of determining whether a product contains vulnerabilities and categorizing potential severity. Organizations seek to adopt and utilize progressive techniques and practices.
						Risk Management: Risk management is the identification, assessment, and prioritization of business, technical, and physical risks as they pertain to the development and deployment of a product. This is followed by a plan to mitigate risks against high priority assets. Threat modeling provides input into risk management practices.
					Plan	**Requirements Management:** Product requirements are documented and traced back to implemented product functionality.
						Industry Best Practice: Trusted technology providers adopt and apply a development/engineering method or process that contributes to the manufacturing of a more secure product.
					Design	**Software/Hardware Design:** Product team documents the design that is intended to meet the stated requirements. An agreement exists between the requirements team and the product development team that documents the acceptance of the design and any stipulations.

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Security Evaluations: Trusted technology providers submit security-enabled products for evaluation under a recognized international standard such as the Common Criteria.
						Industry Best Practice: Trusted technology providers adopt and apply (where applicable) threat and risk models in the design of their product functions and attributes.
					Make	**Lifecycle Automation:** Engineering and/or development practices are automated where possible to ensure consistency, quality, and time-to-market.
						Configuration Management: Product artifacts are managed through version and configuration control and access to source code is protected according to access rights.
						Well-defined Development Process: The overall manufacturing/development process is documented and is inclusive of development partners.
						Run-time Protection Measures: Run-time protection measures include methods to mitigate the impact of vulnerabilities. Such methods include run-time measures that protect executable code against memory space, buffer overflow attacks, null pointers, etc.
					Deliver	**Product Security Configuration:** Product security configuration profile(s) are provided as part of a product distribution. Security configurations are well documented.
					Return	**Product Sustainment Management:** Trusted vendors provide post-GA product support and maintenance in support of their customers. This includes: • A documented feedback and problem reporting process • Customer notification of product defects • Customer notification of exploitable product vulnerabilities • Product remediation as defined by product licensing and well documented customer support agreements
						Product Patching and Remediation: Trusted technology providers have established a well documented and externally visible process for patching and remediating products. Priority is given to known severe vulnerabilities.
					Process Risk Auditing	**Quality/Test Management:** A quality and test product plan exists and testing is conducted according to plan and communicated to management, development partners, and product management.

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
Microsoft	Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity	Process Framework/ Structured Methodologies	Software	Vendor Suppliers	System Lifecycle Integration / Design for Risk	**Standards Correlation Approach:** • Plan • Discover • Assess • Develop • Validate • Implement
						Business Process Model Approach: • Plan • Discover • Assess • Develop • Validate • Implement
Microsoft	Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust	Policy Reform	IT Systems	Governments IT Vendors	System Lifecycle Integration / Design for Risk	**Risk-based Approach:** • Identify key assets • Enumerate threats to those assets • Implement controls to mitigate threats • Establish an incident response procedure • Develop robust threat models • Expand research
						Transparency: Promote transparency
						Flexibility
						Reciprocity
SAFECode	Fundamental Practices for Secure Software Development	Best Practices	Software	Software Developers	System Risk Assessment/ Threat Modeling	Threat Modeling
					Make	Use least privilege
						Sandboxing
						Secure Coding Practices: • Minimize use of unsafe string and buffer functions • Validate input and output to mitigate common vulnerabilities • Use robust integer operations for dynamic memory allocations and array offsets • Use anti-cross site scripting (xss) libraries • Use canonical data formats • Avoid string concatenation for dynamic sol statements • Eliminate weak cryptography • Use logging and tracing
						Testing Recommendations: • Determine attack surface • Use appropriate testing tools • Perform fuzz/robustness testing • Perform penetration testing
SAFECode	Software Integrity Controls	Best Practices	Software	Software Developers Suppliers	System Risk Assessment/ Threat Modeling Sourcing	**Suppliers for vendors should** • Address security threats during design, development, and testing • Assure that the processes to create and deliver products are secure • Make sure their suppliers provide ways to differentiate between genuine and counterfeit products and components

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Vendors Should Have Written Agreements With Suppliers That: • Define expectations • Define intellectual property ownership and responsibilities for protecting the code and development • Understand supplier vulnerabilities and define a response process if vulnerabilities are exploited • Assess supplier's ability to train developers with secure development practices
						Open Source Software: • Controls for more active vulnerability management and incident handling must be implemented • Means to validate the security of open source software must be developed
						TECHNICAL INTEGRITY CONTROLS FOR SUPPLIERS **Secure Transfer:** • Authenticated endpoints • Encrypted for transit • Automate the end-to-end process **Sharing of System and Network Resources:** • Digital identities given to suppliers to access vendor networks should be controlled with limited access only to relevant resources needed • Each resource shared should have an independent assessments as to the authorization required • Supplier's access to vendor resources should expire as soon as the project completes. A fail-safe check should be implemented. A robust procedure using automatic disabling features as well as manual notifications should be used.
						TECHNICAL INTEGRITY CONTROLS FOR SUPPLIERS (continued): **Malware Scanning** • Supplier code should be scanned by the vendor using multiple, up-to-date malware scanning engines. • When possible, suppliers should inform vendors of what scanning has been taken place on the code at their end **Secure Storage** • Code should be stored securely with need-to-know access controls • Transferred code packages should be quickly moved to a secure asset repository **Code Exchange** • Use digitally signed packages and verifiable checksums or hashes • Verify digital signatures with validated time stamps
					Make	**People Security:** • Segregation of duties • Use controlled automated processes • Clearly define roles, responsibilities, and access rights • Management should be aware of who has what access • Train for secure development practices • Train for secure technical controls

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Physical Security: • Building security and access controls should be applied • Security should be periodically reassessed • Code development security should go beyond building security into its own distinct layer of protection
						Network Security: • Network security should be applied using a risk-based process • Session traffic involving source code should be encrypted to acceptable standards • Access to developer workstations should be controlled • Accounts of departing employees should be promptly disabled • Disabled accounts should not be deleted as they can be used for forensic analysis later on • Workstations and virtual machines should be secured to prevent malicious code from being introduced • Developers should have access to the minimum code necessary to complete their task
						Code Repository Security: • All code-related assets should be stored in source code repositories for security and access control • Servers hosting source code should be housed securely • Confidentiality of code should be maintained when kept in separate databases • Systems should be secured in their default state • The default security configuration status should be protected • Access to source code repositories should be controlled through use of corporate identity systems • Change logs for all code modifications should be maintained • A manifest of all code assets of a product should be maintained and managed • Versions of software assets should be tracked with their security characteristics in the repository
						Build Environmental Security • Build environments should be as automated as possible • Traceability of actions on build scripts should be high • Build automation scripts and their changes should be checked into the code repository with the name of the person who makes changes • Service accounts that run in automated fashion between source code repositories and build tools should be traceable to the individuals who execute them
						Peer Review • Use automated tools for scalability • Focus peer reviews on changed code that is scanned again and awaiting approval • Couple peer reviews in relation to exercised code paths in the context of the overall code coverage

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Network Security: • Network security should be applied using a risk-based process • Session traffic involving source code should be encrypted to acceptable standards • Access to developer workstations should be controlled • Accounts of departing employees should be promptly disabled • Disabled accounts should not be deleted as they can be used for forensic analysis later on • Workstations and virtual machines should be secured to prevent malicious code from being introduced • Developers should have access to the minimum code necessary to complete their task
						Code Repository Security: • All code-related assets should be stored in source code repositories for security and access control • Servers hosting source code should be housed securely • Confidentiality of code should be maintained when kept in separate databases • Systems should be secured in their default state • The default security configuration status should be protected • Access to source code repositories should be controlled through use of corporate identity systems • Change logs for all code modifications should be maintained • A manifest of all code assets of a product should be maintained and managed • Versions of software assets should be tracked with their security characteristics in the repository
						Build Environmental Security: • Build environments should be as automated as possible • Traceability of actions on build scripts should be high • Build automation scripts and their changes should be checked into the code repository with the name of the person who makes changes • Service accounts that run in automated fashion between source code repositories and build tools should be traceable to the individuals who execute them
						Peer Review: • Use automated tools for scalability • Focus peer reviews on changed code that is scanned again and awaiting approval • Couple peer reviews in relation to exercised code paths in the context of the overall code coverage

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						TESTING FOR SECURE CODE **Testing Tools:** • Static code analysis tools (source code) • Network and web application vulnerability scanners (dynamic testing) • Binary code analysis tools • Malware detection tools (discover backdoors, etc.) • Security compliance validation tools (hardening, data protection) • Code coverage tools
					Deliver, Return	Malware Scanning
						Code Signing
						Delivery
						Transfer
						Cryptographic Hashed or Digitally Signed Components
						Notification Technology
						Authentic Verification During Program Execution
						Patching
						Secure Configurations
						Custom Code Extensions
Carnegie Mellon	Software Supply Chain Risk Management: From Products to Systems of Systems	Best Practices	Software	Suppliers Acquirers	System Lifecycle Integration/ Design for Risk	**SYSTEM DEVELOPMENT AND INTEGRATION** **Contractors should be able to:** • Analyze software risks associated with the use of commercial products • Manage risk associated with integration of components that have a lower level of assurance than the desired system assurance level • Perform system level attack surface analysis and threat modeling or equivalent practices to identify weaknesses related to how software components are used and integrated into the system • Maintain a staff that has a broad knowledge of exploitable software weaknesses and their mitigation • Test for applicable system development and integration weaknesses as guided by the system's threat model
					System Risk Assessment/ Threat Modeling	**Attack Analysis:** • Attack incentives and enablers • Attack surface • Attacker intent • Risk factors
					Acquisition Risk Assessment/ Sourcing Management	**SUPPLIERS** **Reduce Defects:** **1) Threat Modeling** • Analyze risks • Systematic approach to determining a security model during development • Incorporates detailed flow analysis **2) Testing** • Penetration testing • Fuzz testing- tests with malformed data inputs **Reduce Attack Targets:** **1) Attack Surface Analysis** • Note risks and address them • Partition code to isolate risk

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Supplier Selection: 1) Choose suppliers that are aware of the risks and take measures to mitigate them 2) Supplier risk management certification should look for: • Development staff is knowledgeable in exploitable software weaknesses and trained to mitigate those risks • Physical, personnel, and industrial security measures • Strong configuration management of development facilities • Careful vetting of employees • Assessment and monitoring of their own suppliers and subcontractors • Attack surface analysis and threat modeling or equivalent practices to identify possible software weaknesses and the strength of mitigations needed given the software's indented operational use • Verification that risk mitigation and remediation action are sufficient, that testers are knowledgeable of applicable software weaknesses and mitigations, and that those items are incorporated into the test plan
Carnegie Mellon	Evaluating and Mitigating Software Supply Chain Security Risks	Best Practices	Software	Acquirers Suppliers	Acquisition Risk Assessment/ Sourcing Management	**Using Attack Surface Analysis:** • Perform an initial supply chain security risk assessment • Include supply chain security risk management as part of the RFP • Monitor practices for supply chain security risk management • Assess delivered products/systems • Configure/integrate with consideration of supply chain security risks • Develop user guidance to help mitigate supply chain security risk
						Using Risk Assessment (Threat Modeling): • Write a software supply chain security risk management parts of RFP • Select suppliers that address supply chain security risk • Monitor supply chain security risk management practices • Assess delivered products/systems • Configure/integrate with consideration to supply chain security risks • Monitor component/supplier
					Acquisition Risk Assessment/ Sourcing Management	**Evidence that Required Supplier Security Properties are in Place:** • Architecture and design analysis • Information on development coding practices • The existence of an RFP requirement to provide an attack surface analysis and mitigation plan • Plans to include security testing in acceptance tests • The results of security tests
Carnegie Mellon	A Taxonomy of Operational Cyber Security Risks	Best Practices	IT Systems	Vendor Suppliers	System Risk Assessment/ Threat Modeling	**Actions of People:** • Inadvertent • Deliberate • Inaction
						Systems and Technology Failures: • Hardware • Software • Systems

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Failed Internal Processes • Process design or execution • Process controls • Supporting processes
						External Events • Disasters • Legal issues • Business issues • Service dependencies
NIST	NIST IR 7622 (preliminary draft)	Best Practices	IT Systems	Acquirers Integrators Suppliers	Executive Risk/Governance Group	• Develop procedures for implementing ICT SCRM mitigation strategies • Create a diverse cross enterprise group for Risk Management governance
					Extended Enterprise Risk Mitigation Strategy	Establish a coordinated team approach to assess the ICT supply chain risk
					System Lifecycle Integration	• Automating methods for managing and verifying the configuration • Backing up of the configuration management System • Recovery process for the system failure/breach
					System Risk Assessment	• Use technical and programmatic mitigation techniques • Create Standard operation procedure for determining risk impacts; refer NIST SP 800-53 for controls
					Acquisition Risk Assessment	FIPS 199 High impact systems, ICT SCRM should be integrated into the acquisition process
					Supply Chain Network Modeling	• Uniquely Identify and Label Supply Chain Elements, Processes, and Actors • Create and Maintain the Provenance of Elements, Processes, Tools and Data • Limit Access and Exposure within the Supply Chain
					Tracking and Visibility of Supply Chain Components	Employ tools and techniques to determine if authenticators are sufficiently strong to resist attacks intended to discover or compromise authenticators
					Program/ Project/etc Auditing/ Monitoring	• Review of the CM processes • Share information with strict limits
					Plan	Performance based contracts. e.g., requests for quotation (RFQ), requests for proposal (RFP)
					Design	• Identifying and gathering information on the supplier/integrator organization • Robustness and completeness of life cycle processes applied to elements and services to be procured • Conduct Security, Threat, and Vulnerability Assessment
					Deliver	• Manage Disposal and Final Disposition Activities Throughout the Lifecycle • Strengthen Delivery Mechanisms
					Return	Develop organizational policy and procedures that require that any counterfeit/grey market parts detected will be seized, destroyed, or preserved for law enforcement evidentiary purposes
					Process Risk Auditing	• Audit integrators' ability to trace critical elements and processes throughout the supply chain • Share the audits information with the stakeholders

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
NIST	Piloting Supply Chain Risk Management Practices for Federal Information Systems (final version)	Best Practices	IT Systems	Acquirers Integrators Suppliers	System Lifecycle Integration / Design for Risk	Enable Diversity
						Identify and Protect Critical Processes and Elements
						Protect the Supply Chain Environment
						Configure Elements to Limit Access and Exposure
						Formalize Service/Maintenance
						Manage Configuration
						Consider Personnel in the Supply Chain
						Promote Awareness, Educate, and Train Personnel on Supply Chain Risk
						Negotiate Requirements Changes
						Incorporate Supply Chain Assurance in Requirements
						Use Defensive Design for Elements, Processes and Organizations
					Acquisition Risk Assessment/ Sourcing Management	Maximize Acquirer's Visibility into Integrators and Suppliers
						Protect Confidentiality of Element Uses

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Select Trustworthy Elements
					Program/ Project/Process Risk Auditing/ Monitoring	Manage Supply Chain Vulnerabilities
						Respond To Supply Chain Incidents
						Test Throughout The System Development Lifecycle
					Deliver	Reduce Supply Chain Risks During Disposal
						Harden Supply Chain Delivery Mechanisms
					Return	Reduce Supply Chain Risks During Software Updates And Patches
					Process Risk Auditing	Protect/Monitor/Audit Operational System
NIST	Risk Management Guide for Information Technology Systems	Best Practices	IT Systems	Supplier Vendors	System Lifecycle Integration / Design for Risk	**Risk Mitigation Options:** • Risk assumption • Risk avoidance • Risk limitation • Risk planning • Research and acknowledgment • Risk transference
						Approach for Control Implementation: Step 1: Prioritize actions Step 2: Evaluate recommended control options Step 3: Conduct cost-benefit analysis Step 4: Select control Step 5: Assign responsibility Step 6: Develop a safeguard Implementation plan Step 7: Implement selected controls
						Control Categories: • Technical security controls • Management security controls • Operational security controls
						Cost-Benefit Analysis of Resource Allocation for Security Controls
					System Risk Assessment/ Threat Modeling	**Risk Assessment:** Step 1: System Characterization Step 2: Threat Identification Step 3: Vulnerability Identification Step 4: Control Analysis Step 5: Likelihood Determination Step 6: Impact Analysis Step 7: Risk Determination Step 8: Control Recommendations Step 9: Results Documentation
NIST	Contingency Planning Guide for Information Technology Systems	Best Practices	IT Systems	Supplier Vendors	System Lifecycle Integration / Design for Risk	**IT Contingency Planning Process:** • Develop the contingency planning policy statement • Conduct the business impact analysis • Identify preventive controls • Develop recovery strategies • Develop an IT contingency plan • Plan testing, training, and exercises • Plan maintenance
						IT Contingency Plan Development: • Supporting information • Notification/activation phase • Recovery phase • Reconstitution phase • Plan appendices

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Technical Contingency Planning Considerations: • Desktop computers and portable systems • Servers • Web sites • Local area networks • Wide area networks • Distributed systems • Mainframe systems
NIST	Guide to Selecting Information Technology Security Products	Best Practices	IT Systems	Suppliers, Acquirers	Acquisition Risk Assessment/ Sourcing Management	Identification and Authentication
						Access Control Enforcement
						Intrusion Detection
						Firewall
						Public Key Infrastructure
						Malicious Code Protection
						Vulnerability Scanners
						Forensics
						Media Sanitizing
NIST	Recommended Security Controls for Federal Information Systems	Best Practices	IT Systems	Supplier	System Lifecycle Integration / Design for Risk	Categorize the information system and the information processed, stored, and transmitted by that system based on a FIPS 199 impact analysis.
						Select an initial set of baseline security controls for the information system.
						Implement the security controls and describe how the controls are employed within the information system and its environment of operation.
						Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.
						Authorize information system operation based on a determination of the risk.
						Monitor the security controls in the information system on an ongoing basis.
Internet Security Alliance	The ISA Guidelines for Securing the Electronic Supply Chain	Best Practices	Hardware	Supplier Acquirer	Plan, Design	• General product design • Modularization of product design • Schematic product design • Physical product design • Creation and evaluation of product prototypes • Creation of templates and molds for the non-electronic components • Consolidation and clean-up of design process information
					Make (Photomask Production Phase)	• Wafer mask receiving • Wafer mask production process • Wafer mask production personnel • Management of finished masks

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
					Source, Make, Deliver (Microelectronic Fabrication Phase)	• Microelectronic fabrication sourcing and receiving • Microelectronic fabrication process • Personnel in microelectronic fabrication • Microelectronic fabrication quality control and verification tests • Chip package assembly and downloading of firmware
					Source, Make, Deliver (Circuit Board Fabrication Phase)	• Sourcing and receiving of circuit board materials • Receiving and tooling of circuit board designs • Circuit board fabrication process • Circuit board fabrication personnel • Circuit board quality control and testing • Circuit board shipping
					Source, Make, Deliver (The Board Pre-Assembly Phase)	• Pre-assembly sourcing and receiving • Processes in the pre-assembly facility • Personnel in pre-assembly • Shipping of circuit boards to assembly facility
					Source, Make, Deliver (Product Assembly Phase)	• Assembly sourcing and receiving • Product assembly processes • Personnel in product assembly • Product assembly testing and repairs • Product assembly outputs
					Deliver (Product Distribution Phase)	• Secure receiving and storage of product shipments • Breakdown into individual product orders • Management of product sales force • Management of relationships with middlemen • End-user delivery and registration
					Return (Product Maintenance Phase)	• Training of product maintenance personnel • Updates to product • Servicing of product • Disposal of used products
					Legal (Necessary Legal Conditions)	• National laws and legal framework • The nature of the corporate relationships • Police and criminal courts
Intel and Cisco	Common Criteria Embrace, Reform, Extend	Policy Reform	Software Hardware Firmware	Technology Vendors, IT Product Security Evaluators	System Risk Assessment/ Threat Modeling	• Use the Common Criteria Forum (CCF) to create an organization that is a standard body to ensure the reform goals are met • Establish and work through Common Criteria • Technical Communities • Accelerate and enhance Protection Profile (PP) development • Improve Evaluation Efficacy • Expand CC to address manufacturing process integrity aspects of supply chain
Common Criteria/ Microsoft	Customer Perceptions about the Relevancy of Common Criteria for Supply Chain Security	Policy Reform	Software	Software developers	System Risk Assessment/ Threat Modeling	Protection Profiling and Threat Modeling
						Common Criteria Management Requirements: • Production support • Acceptance procedures • Automation
						Site Certification
NIAP	Untitled Common Criteria Document	Policy Reform	Information Technology Systems	Governments Companies	System Risk Assessment/ Threat Modeling	Reform Common Criteria for the IT Supply Chain

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
Common Criteria	A CC Community for Supply Chain	Policy Reform	Hardware Software	Vendors Suppliers Risk Evaluators	System Risk Assessment/ Threat Modeling	Establish supply chain community Common Criteria Community
Global Innovation and Strategy Center	U.S. Reliance on Foreign IT: Mitigating Risks Associated with Foreign Sources of Hardware Components	Policy Reform	Hardware	Government Vendor Suppliers	Plan, Source, Make (Government Policies)	**Controlling Hardware Supplies:** • Economic Incentives for Domestic Design • Trusted Foundries • Import and Acquisition Regulations • Longevity of Trust-Based Solutions
						Developing Intellectual Assets: • Education Initiatives • Geek Culture Outreach
					Make, Deliver	Side-Channel Verification
						Physical Unclonable Functions (PUFs)
						Radio Frequency Identification (RFID) and Tracking
						Implementation of Technological Solutions
Telecom Carrier Working Group	Foreign Supply Chain Security Risk Management: A Proposed Model, Protecting the U.S. Public Telecommunica-tions Network Infrastructure	Process Framework/ Structured methodolo-gies Policy Reform	Telecomm Networks	Government Telecommuni-cations Council Foreign suppliers Third Party Security Evaluators Suppliers	Enterprise Risk Assessment	**Vulnerability Analysis:** • Interfaces across management, control and user planes • Product security features • Source code analysis • Product releases, patches and field maintenance processes and handoffs • Product development environment • Supply chain and third party product and component integration • Testing software, hardware, and firmware of Element Management Systems and Network Elements
					Enterprise Risk Mitigation Strategy	**Risk Mitigation Initiatives:** • Procedural • Contractual • Physical • Technical

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
ISO/IEC 27036 Standard	ICT SCRM- ISO Standards Update	Formal Standards		Acquirers, Vendor Suppliers	Acquisition Risk Assessment/ Sourcing Management	This standard is in a Working Draft stage; content is still being added by national member bodies. The intent of the overall multipart standard is to address all aspects of information security in supplier relationships which covers most of the tiers of your framework. Currently not all the attributes are covered in the current versions of the documents but national bodies and non-profits believe that governance issues will be addressed in future reviews and they will provide content to fill that gap. Brief summary of what the standard is supposed to provide: • Part 1 provides an overview of the problem of securing information in supplier relationships. This covers any supplier relationship which is broader than ICT SCRM. This is a short document that includes definitions, introduction of the problem, and overall structure of the multipart standard. • Part 2 provides specific requirements that would apply to any supplier relationship and will provide requirements for suppliers and acquirers to assure information security of both parties in a supplier relationship. This document will include additional requirements within ISO/IEC 15288 lifecycle processes (new clause 6) for managing multiple suppliers (supplier inventory and registry, risk assessment, risk management, overall requirements for information security, etc.). Please note that LIFECYCLE PROCESSES are not equal to LIFECYCLE. These are the processes that can be used in multiple phases of any lifecycle and are based on ISO/IEC 15288 lifecycle processes. This standard will ALSO include a generic supplier relationship lifecycle (current clause 6 to become clause 7) that provides requirements for information security within a context of establishing a single supplier relationship. All requirements in this document are expected to be general and high-level. • Part 3 provides guidance on specific ICT SCRM requirements which will augment the general requirements in Part 2. It is structured along ISO/IEC 15288 lifecycle processes as well and will be more technical than Part 2, as well as specific to ICT. Some general content that is in the current attached version of Part 3 will migrate into Part 2 to serve as the foundation for the new Clause 6 in Part 2. • Part 4 which is currently not being developed is meant to provide guidance on specific security requirements related to outsourcing. This is expected to look similar to Part 3 in terms of augmenting general requirements in Part 2 but will address outsourcing. • Part 5 will address specific requirements that address information security for supplier relationships within the context of cloud computing.

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
Booz Allen Hamilton	ICT SCRM- ISO Standards Update	Formal Standards			Make, Source, Deliver (standards development)	**ISO Standards Development Process:** • Begins with an established marketplace requirement that is communicated through a national standards body, which proposes the request to a corresponding subcommittee • The subcommittee presents the proposal for a discussion and a vote, and, if accepted, the subcommittee begins working on the standard • An editor is sought and provided--an expert who leads the standard's development • The subcommittee reviews multiple drafts and requests comments from national standards bodies and liaison organizations to advance drafts to the next formal stage of development • Advancing the standard from one formal stage to another requires an international ballot, voted on by each standards body, one vote per country • With their vote, the national standards bodies submit comments on content, suggestions for improvement, and explanations for no votes • When a standard successfully advances through all required stages, it is published as an international standard
Department of Defense	ISO/IEC 27036	Formal Standards			Make, Source, Deliver (standards development)	**Objectives/Scope:** Develop a globally accepted (commercial) standard to specify requirements and guidance for managing supplier relationships to address all types of organizations and all types of supplier relationships, including outsourcing, product and service acquisition, and cloud computing.
Department of Defense	Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program	Best Practices	IT Supply Chain	Suppliers Acquirers	Extended Risk Assessment	The document addresses: hardware, software, and organizations involved throughout the supply chain. For each of the 32 key practices, there are, in fact four sets of practitioners (communities of practice) that deal with different facets of the same set of supply chain risk problems or apply common tools to different features of the risk set as follows: • Acquisition community including Milestone Decision Authorities (Corporate and Government Executives), their staffs, and all of the folks involved in acquisition and procurement planning. • The Systems Engineering community of practice which spans R,D,T,E as well as prototyping for use, prototyping for manufacturing, assembly and manufacture, packaging for use, packaging for delivery, field sustainment, depot sustainment, retirement and disposal. • The Compliance community of practice which can overlap with the acquisition community and systems engineering community and ensures that suppliers and consumers fulfill their obligations ranging from compliance with law, regulation, and contract, to specific compliance with internal controls and internal corporate entity processes • The security community which includes but is not limited to physical security, information security, personnel security, industrial security, and information assurance and may extend to include law enforcement and intelligence individuals and organizations.

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
					Enterprise Risk Mitigation Strategy	Diversify
						Protect Confidentiality of Users and Uses
						Protect Critical Elements and Processes
						Protect The SC Environment
						Formalize Service/Maintenance
						Ensure Trustworthiness Of Personnel In SC
						Constrain Roles To Limit SC Adverse Consequences
						Promote Awareness, Educate, and Train Personnel on Supply Chain Risks
						Incorporate SC Issues in Risk Management
					System Lifecycle Integration/ Design for Risk	Use Defensive Design
						Use/Create Standard Interfaces to Increase Supplier Diversity

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Choose Programming Languages/Subsets/Tools That Counter Weaknesses
						Configure Elements to Limit Access and Exposure
						Perform Configuration Management
					Acquisition Risk Assessment/ Sourcing Management	Maximize Acquirer's Visibility into Suppliers
						Select Trustworthy Elements
						Evaluate Supplier and Their Supply Chain
						Manage SC Risks Through All Acquisition and Project Processes
						Negotiate Requirements Changes
						Collaboratively Develop/Maintain Trustworthy Elements
					Program/ Project/Process Risk Auditing/ Monitoring	Perform Penetration Testing
						Protect/Monitor/Audit System During All Operations
						Perform Manual Review of Elements, Processes, and Information
						Perform Static Analysis of Elements, Processes, and Information
						Perform Dynamic Analysis of Elements, Processes, and Information (Including Fuzz Testing)
						Manage SC Vulnerability
						Manage SC Incidents
						Continue ICT SCRM Throughout Sustainment
					Deliver	Reduce SC Risks During Disposal
						Harden SC Delivery Mechanisms
					Return	Reduce SC Risks During Software Updates and Patch Management
Department of Homeland Security	Architecture and Design Considerations for Secure Software	Best Practices	Software	Acquirers Vendor Suppliers	System Lifecycle Integration/ Design for Risk	**Software Design Products:** • Models, prototypes, and simulations, and their related documentation • Preliminary user's manual • Preliminary test requirements • Documentation of feasibility • Documentation of the traceability of requirements to the architecture design
						Abstraction: A process for reducing the complexity of a system by removing unnecessary details and isolating the most important elements to make the design more manageable
						Decomposition: The process of describing the generalizations that compose an abstraction
						Minimize the number of high-consequence targets: • Principle of least privilege • Separation of privileges, duties, and roles • Separation of domains

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Don't Expose Vulnerable or High-Consequence Components: • Keep program data, executables, and configuration data separated • Segregate trusted entities from untrusted entities • Minimize the number of entry and exit points • Assume environment data is not trustworthy • Use only trusted interfaces to environment resources
						Deny Attackers the Means to Compromise: • Simplify the design • Hold all actors accountable • Timing, synchronization, and sequencing should be simplified to avoid issues • Make secure states easy to enter and vulnerable states difficult to enter • Design for controllability • Design for secure failure
						Economy of Mechanism: Keep the design as simple and small as possible
						Fail-safe Defaults: Base access decisions on permission rather than exclusion
						Complete Mediation: Every access to every object must be checked for authority
						Open Design: The design should not be secret
						Separation of Privilege: A protection mechanism that requires two keys to unlock is more robust and flexible than one that allows access to the presenter with only a single key
						Least Privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job
						Least Common Mechanism: Minimize the amount of mechanism common to more than one user and depended on by all users
						Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly
						Secure Design Patterns • Distrustful decomposition • Prvilege separation • Defer to restricted application or area
						Design-level Patterns: • Secure state machine • Secure visitor
						Multiple Independent Levels of Security: and Safety: • Data separation • Information flow • Sanitization • Damage limitation

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
					System Risk Assessment/ Threat Modeling	**Threat Modeling:** • Decomposing: understand, through a process of manual inspection, how the application works, its assets, functionality, and connectivity • Defining and classifying the assets: classify the assets into tangible and intangible assets and rank them according to business importance • Exploring potential vulnerabilities: whether technical , operational, or managerial • Exploring potential threats: develop a realistic view of potential attack vectors from an attacker's perspective, by using threat scenarios or attack trees • Creating mitigation strategies: develop mitigating controls for each of the threats deemed to be realistic
					Design	**Architecture Phase:** • Control filenames • Enforce boundaries • Place server-side checks • Generate errors upon suspicion of attack • Provide orderly resource-shutdown • Protect against inappropriate initialization • Restrict executables
						Design Phase: • Preserve OS command structure • Use modular cryptography • Encrypt data with a reliable encryption scheme before transmitting sensitive information • Specify the download of code only after integrity check • Protect against denial of service attacks • Protect against CSRF • Authenticate • Preserve web page structure to mitigate risk from cross-site scripting
					Make	**Secure Session Management:** • Session IDs should be created with the same standards as passwords • Session IDs, like all sensitive data, should be transmitted by secure means and stored in a secure location • The application should check that all Session IDs being used were originally distributed by the application server
Software Security Testing	Best Practices	Software	Acquirers Vendor Suppliers	Acquirers Vendor Suppliers	Process Risk Auditing	**What to Test:** • People; to ensure that there are adequate education and awareness • Processes; to ensure that there are adequate policies and standards and that people know how to follow these policies • Technology; to ensure that the processes have been effective in their implementation
						Test plans include: • Security test cases and scenarios based on the misuse/abuse cases • Test data (both meaningful and fuzzed) • Identification of the test tools and integrated test environment or "ecosystem" • Pass/fail criteria for each test • Test report template. This should enable capture and analysis of test results and of actions for addressing failed tests
						Requirements Specification: • Misuse/abuse cases • Attack models

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Design: • Design Review • Risk Analysis • Formal Proofs
						Implementation: • Code Review • Compile-time Detection • Static Analysis Fault • Injection • Fuzz Testing • Binary Code Analysis • Vulnerability Scanning
						Verification: • Static Analysis • Source Code Fault Injection • Binary Fault Injection • Fuzz Testing • Binary Code Analysis • Vulnerability Scanning • Penetration Testing
						Deployment and Sustainment: • Static Analysis • Vulnerability Scanning • Impact Analysis • Regression Testing
						Risk Analysis: • Decomposing the application • Defining and classifying the assets • Exploring potential vulnerabilities • Exploring potential threats • Creating mitigation strategies
						Code Review
						Automated Static Analysis
						Source Code Fault Injection
						Binary Fault Injection
						Fuzz Testing
						Binary Code Analysis
						Vulnerability Scanning
						Penetration Testing
Department of Homeland Security	Secure Coding	Best Practices	Software	Acquirers Vendor Suppliers	Plan, Design	**Preparing to Write Secure Code:** • Choose a language with security in mind • Create a secure development environment • Create an application guide • Identify safe and secure software libraries
					Make	**Secure Coding Principles:** • Keep code small and simple • Make code backward and forward traceable • Code for reuse and maintainability • Follow secure coding standards and/or guidelines • Use compiler security checking and enforcement • Avoid security conflicts arising between native and non-native, passive, and dynamic code • Review code during and after coding

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Secure Coding Practices: • SANS Top 25 Error List/OWASP Top 10 List • Validate and encode input • Filter and sanitize output and callouts • Minimize retention of state information • Do not allow unauthorized privilege escalation • Leverage security through obscurity only as an additional deterrence measure • Incorporate interprocess authentication • Leverage attack patterns • Implement encryption and hashing • Disable debugging tools prior to deployment
						Secure Memory and Cache Management • Limit persistent memory caching • Allocate memory and other resources carefully
						Secure Error and Exception Handling: • Integrate anomaly awareness • Incorporate runtime error checking and safety enforcement • Use event monitors
Department of Homeland Security	Requirements and Analysis for Secure Software	Best Practices	Software	Acquirers Vendor Suppliers	System Risk Assessment/ Threat Modeling	**Eliciting Security Requirements:** • Misuse/Abuse Cases • Threat Analysis • Soft Systems Methodology • Quality Function Deployment • Controlled Requirements Expression • Issue-based Information Systems • Joint Application Development • Feature-oriented Domain Analysis • Critical Discourse Analysis • Accelerated Requirements Method
						Approaches to Security Requirement Development: • The Comprehensive, Lightweight Application Security Process • Security Quality Requirements Engineering • Core Security Requirements Artifacts
						Requirements Prioritization Methods: • Binary Search Tree • Numeral Assignment Technique • Planning Game • The 100-Point Method • Theory-W • Requirements Triage • Wiegers' Method • Analytic Hierarchy Process • Requirements Prioritization Framework
Department of Homeland Security	Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses	Best Practices	Software	Acquirers Vendor Suppliers	Plan, Design	**REQUIREMENTS, ARCHITECTURE, AND DESIGN PHASES** **Prevention and Mitigation Practices for:** • Improper Input Validation • Improper Encoding or Escaping of Output • Failure to Preserve SQL Query Structure • Failure to Preserve Web Page Structure • Failure to Preserve OS Command Structure • Cleartext Transmission of Sensitive Information • Cross-Site Request Forgery • Race Condition • Failure to Constrain Operations within the Bounds of a Memory Buffer • External Control of Critical State Data • External Control of File Name or Path

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
						Prevention and Mitigation Practices for (continued): • Untrusted Search Path • Failure to Control Generation of Code • Download of Code Without Integrity Check • Improper Resource Shutdown or Release • Improper Initialization • Improper Access Control • Use of a Broken or Risky Cryptographic Algorithm • Hard-Coded Password • Insecure Permission Assignment for Critical Resource • Use of Insufficiently Random Values • Execution with Unnecessary Privileges • Client-Side Enforcement of Server-Side Security
					Make	**BUILD, COMPILATION, IMPLEMENTATION, TESTING, AND DOCUMENTATION** **Prevention and Mitigation Practices for:** • Improper input validation • Improper encoding or escaping of output • Failure to preserve SQL query structure • Failure to preserve web page structure • Failure to preserve OS command structure • Cleartext transmission of sensitive information • Cross-site request forgery • Race condition • Error message information leak • Client-side enforcement of server-side security • Failure to constrain operations within the bounds of a memory buffer
						Prevention and Mitigation Practices for (continued): • External control of critical state data • External control of file name or path • Untrusted search path • Failure to control generation of code • Download of code without integrity check • Improper resource shutdown or release • Improper initialization • Incorrect calculation • Use of a broken or risky cryptographic algorithm • Improper access control • Insecure permission assignment for critical resource • Use of insufficiently random values • Hard-coded password • Execution with unnecessary privileges
						INSTALLATION, OPERATION, AND SYSTEM CONFIGURATION PHASES **Prevention and Mitigation Practices:** • Failure to preserve SQL query structure • Failure to preserve web page structure • Failure to preserve OS command structure • External control of critical state data • Cleartext transmission of sensitive information • Error message information leak • Failure to constrain operations within the bounds of a memory buffer • External control of file name or path • Failure to control generation of code • Improper access control • Insecure permission assignment for critical resource

Detailed Matrix of ICT SCRM Initiatives, Cont.

Document Author	Document Name	Purpose	IT Components	Key Actors	Framework Attributes Addressed	Risk Management Practices
Department of Homeland Security	Software Supply Chain Risk Management and Due-Diligence	Best Practices	Software	Acquirers Vendor Suppliers	Program/ Project/Process Risk Auditing/ Monitoring	**Software Assurance Concern Categories:** • Software History and Licensing • Development Process Management • Software Security Training and Awareness • Planning and Requirements • Architecture and Design • Software Development • Built-in Software Defenses • Component Assembly
						Software Assurance Concern Categories (continued): • Testing • Software manufacture and packaging • Installation • Assurance claims evidence • Support • Software change management • Timeliness of vulnerability mitigation • Individual malicious behavior • Security "track record" • Financial history and status • Organizational history • Foreign interest and influences • Service confidentiality policies • Operating environment for services • Security services and monitoring
Department of Homeland Security	Software Assurance in Acquisition and Contract Language	Best Practices	Software	Acquirers Vendor Suppliers	System Risk Assessment/ Threat Modeling	**Contract Phase:** • Work statement • Instructions to offerors/suppliers • Terms and conditions • Certifications • Prequalification • Proposal evaluation • Contract negotiation and contract award
						Monitoring and Acceptance Phase: • Contract work schedule • Change control • Review and acceptance of software deliverables • Risk management • Assurance case management • Independent software testing
						Follow-on Phase: • Sustainment (post-release support) • Risk management • Assurance case management/transition to operations • Change management • Disposal or decommissioning
Department of Homeland Security	Software Assurance in Education, Training and Certification	Best Practices	Software	Acquirers Vendor Suppliers	System Risk Assessment/ Threat Modeling	**Software Assurance Education:** • Tools • Books • Standards of practice • Workforce credentials • Vendors • Role descriptions

Document List

Doc #	Author	Title
1	SAFECode	Fundamental Practices for Secure Software Development 2nd Edition
2	SAFECode	Software Integrity Controls
3	SAFECode	The Software Supply Chain Integrity Framework
4	Internet Security Alliance	The ISA Guidelines for Securing the Electronics Supply Chain (Draft Version 6)
5	Carnegie Mellon	Software Supply Chain Risk Management: From Products to Systems of Systems
6	Carnegie Mellon	Evaluating and Mitigating Software Supply Chain Security Risks
7	Carnegie Mellon	A Taxonomy of Operational Cyber Security Risks
8	NIST	Guide to Selecting Information Technology Security Products
9	NIST	NIST IR 7622(draft)
10	NIST	Piloting Supply Chain Risk Management for Federal Information Systems
11	NIST	Contingency Planning Guide for Information Technology Systems
12	NIST	Risk Management Guide for Information Technology Systems
13	NIST	An Introduction to Computer Security: The NIST Handbook
14	NIST	Security Considerations in the System Development Life Cycle
15	NIST	Recommended Security Controls for Federal Information Systems
16	Microsoft	Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust
17	Microsoft	Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity
18	Telecom Carrier Working Group	Foreign Supply Chain Security Risk Management: A Proposed Model, Protecting the U.S. Public Telecommunications Network Infrastructure
19	The Open Group	Open Trusted Technology Provider Framework (O-TTPF)
20	Global Innovation and Strategy Center	US Reliance on Foreign IT, Mitigating Risks Associated with Foreign Sources of Hardware Components
21	NIAP	CC - Community NIAP Vision 11-10
22	NIAP	Customers Perceptions about the Relevancy of Common Criteria for Supply Chain Security
23	NIAP	A CC Community for Supply Chain
24	Intel and Cisco	Common Criteria, Embrace Reform Extend
25	Department of Defense	Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program
26	Supply Chain Council	Supply Chain Operations Reference (SCOR) model Overview - Version 10.0
27	UMD and SAIC	Building a Cyber Supply Chain Assurance Reference Model
28	UMD	Toward a Cyber-Supply Chain Code of Practice
29	Homeland Security	Supply Chain Risk Management
30	LMI	Using the SCOR Model for Supply Chain Risk Management
31	LMI	IR10J Cyber Supply Chain Security, Final Briefing
32	LMI	IR10J Cyber Supply Chain Security, Final Detail Briefing
33	Tuck School of Business at Dartmouth	Making Information Risk Mitigation Decisions
34	Vanany, Zailani, Pujawan	Supply Chain Risk Management: Literature Review and Future Research

Document List, cont.

Doc #	Author	Title
35	Department of Defense	Acquisition of Information Technology
36	Gordon, Martin, UMD	The Economics of Information Security Investment
37	Ross Anderson	The Economics of Information Security
38	Kjell Hausken	Information Sharing Among Firm and Cyber Attacks
39	Eric Rescorla	Is Finding Security Holes a Good Idea?
40	Center for Digital Strategies, Tuck School of Business, Dartmouth College	Managing Information Risk and the Economics of Security
41	Cavusoglu, Mishra, Raghunathan	The Value of Intrusion Detection Systems in Information Technology Security Architecture
42	Bauer, van Eeten	Cybersecurity: Stakeholder incentives, externalities, and policy options
43	GW Cyber Security Policy and Research Institute	An Overview of the Economics of Cybersecurity and Cybersecurity Policy
44	Carnegie Mellon	Enterprise Information Security: Who should manage it and how?
45	President's Information Technology Advisory Committee	Cyber Security: A Crisis of Prioritization
46	CSI/FBI	Computer Crime and Security Survey
47	United States Institute of Peace	Cyber Terrorism, How Real Is the Threat?
48	European Commission	EU Policy on Network and Information Security and Critical Information Infrastructures Protection
49	Intelligence and National Security Alliance	Critical Issues for Cyber Assurance Policy Reform
50	Information Assurance Technology Analysis Center	Measuring Cyber Security and Information Assurance
51	Information Assurance Technology Analysis Center	Software Security Assurance
52	Center for Digital Strategies, Tuck School of Business	Information Security and Privacy in Healthcare: Current State of Research
53	International Telecommunication Union	A Comparative Analysis of Cybersecurity Initiatives Worldwide
54	JASON	Science of Cyber-Security
55	Homeland Security	A Roadmap for Cybersecurity Research
56	European Network and Information Security Agency	Inter-X: Resilience of the Internet Interconnection Ecosystem
57	MITRE	Cyber Security Governance
58	Department of Homeland Security	Software Assurance in Education, Training and Certification
59	Department of Homeland Security	Software Security Testing
60	Department of Homeland Security	Secure Coding
61	Department of Homeland Security	Requirements and Analysis for Secure Software
62	Department of Homeland Security	Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
63	Department of Homeland Security	Software Supply Chain Risk Management and Due-Diligence
64	Department of Homeland Security	Software Assurance in Acquisition and Contract Language
65	Department of Homeland Security	Architecture and Design Considerations for Secure Software
66	International Standards Organization	ISO/IEC JTC 1/SC 27 - N10131 - 270361 - N9965
67	International Standards Organization	ISO/IEC JTC 1/SC 27 - N10XXX - 270362 - N9967
68	International Standards Organization	ISO/IEC JTC 1/SC 27 - N10133 - 270363 - N9969

APPENDIX 4

Emerging ICT SCRM Consensus Areas

	Open Group	ISA	ISO 27036	NIST
Key Practices	• Trusted technology providers apply well-formed and documented development (or manufacturing) method or process. • Product engineering methods are specified and refined to best fit the engineering/ development characteristics of the target product. • Supply chain security and integrity is treated as a key element of the end-to-end development/manufacturing process. • Trusted technology providers select suppliers who follow equivalent secure development/engineering practices for supplied components and follow hardening practices to secure their configuration.	NA	• Part 1 provides an overview of the problem of securing information in supplier relationships. • Part 2 provides specific requirements that would apply to any supplier relationship and will provide requirements for suppliers and acquirers to assure information security of both parties in a supplier relationship. • Part 3 provides guidance on specific ICT SCRM requirements which will augment the general requirements in Part 2.	• Maximize acquirer's visibility into integrators and suppliers • Manage supply chain vulnerabilities • Harden supply chain delivery mechanisms
Processes	• Product lifecycle practices and processes are supported by a community of practitioners who vigilantly maintain the organization's engineering practices. • Product requirements are documented and traced back to implemented product functionality. • Product team documents the design that is intended to meet the stated requirements • Engineering and/or development practices are automated where possible to ensure consistency, quality, market.	• Modularization/Schematic/ Physical product design • Creation and evaluation of product prototypes • Creation of templates and molds for the non-electronic components • Consolidation and clean-up of design process information.	• Subcommittee presents the proposal for a discussion and a vote, and works when accepted • An editor, who is an expert leads the standard's development • The proposal advanced to next stage after seeking reviews and recommendations from multiple national/ international standards bodies and liaison organizations • When a standard successfully advances through all required stages, it is published as an international standard.	• Manage disposal and final disposition activities throughout the lifecycle • Harden supply chain delivery mechanisms
Technology	• Threat models are used as input to the creation of test plans and cases. • Validation technology is embedded into the trusted supply chain. • Testing is conducted according to quality and test product plan and communicated to management, development partners, and product management.	• Stress on Microelectronics fabrication sourcing and receiving and other processes • Stress on Microelectronics fabrication quality control and verification tests • Ensure security during Chip package assembly and downloading of firmware	NA	• Testing done throughout the system development lifecycle • Stress on Reduction in supply chain risks during software updates and patches • Technical Contingency Planning Considerations given preference.

For further information, please contact the Principal Investigator:

Dr. Sandor Boyson
Supply Chain Management Center
University of Maryland
College Park, MD 20742-1815
301.405.2205 Tel
301.509.4880 Mobile
sboyson@rhsmith.umd.edu
www.rhsmith.umd.edu

"For Peace and Harmony Across the ICT SCRM Galaxy"

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS