



Assessing Supply Chain Risks to Inform Risk-Response and Action

Angela Smith
Computer Security Division
IT Laboratory

C3E Symposium 2021
October 28, 2021

NIST's Cybersecurity-SCRM Program



GUIDANCE



COLLABORATION



RESEARCH

NIST Approach: Holistic in Breadth and Depth

System Development Life Cycle:

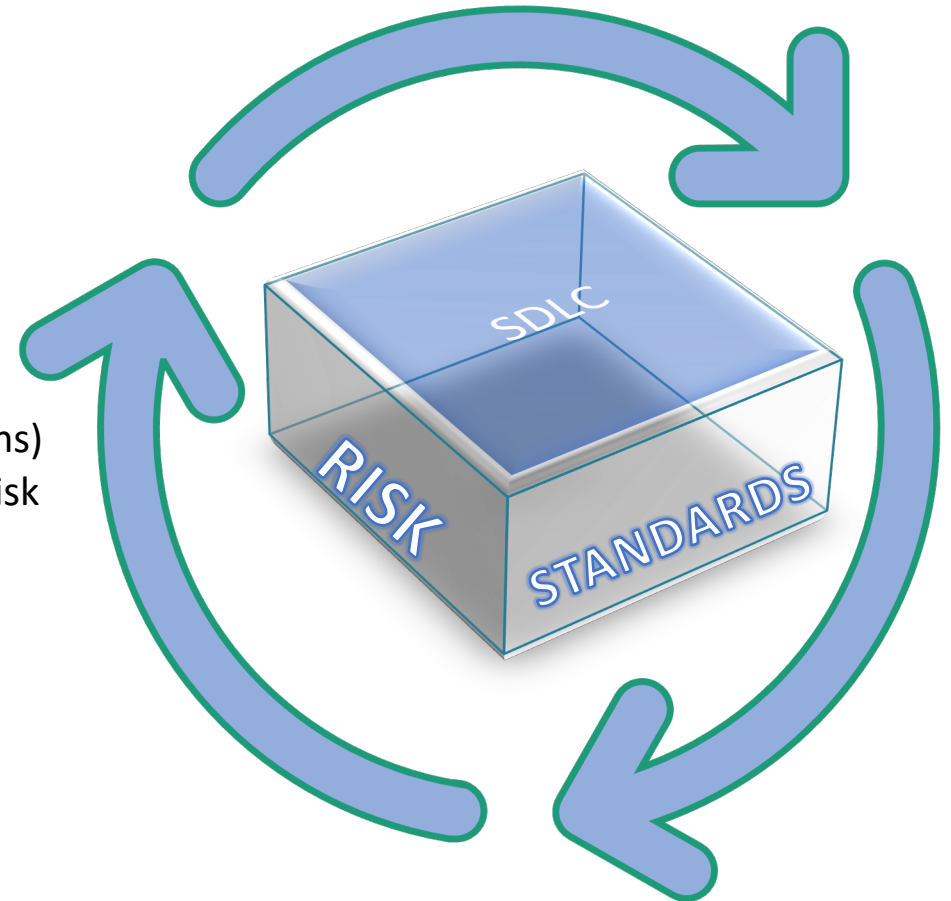
- design, development, acquisition/procurement, delivery, installation, integration, operations & maintenance, and disposal/retirement

Risk-Based Perspective

- Organization Layers: Enterprise, Mission/Business, Operational
- Criticality (Systems/Technology, Suppliers, Data, Mission/Business Functions)
- Frame Risk (Understand Context), Assess Risk, Respond to Risk, Monitor Risk

External Standards and Practices

- Managerial (e.g. Policy, Processes, Plans) and Technical Controls (e.g. Configurations, Access Rights)
- Best practices; Assurance Frameworks; Automation/Tools, etc.



NIST C-SCRM Program Products

- NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems (2012)
- SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organization (2015)
- Integrating C-SCRM into pubs:
 - CSF v1.1 (2017);
 - SP 800-37 Revision 2 (2018);
 - SP 800-53 Revision 5 (2020); SP 800-53B (2020); and IPD SP 800-53A (Summer 2021)
- - NISTIR 8179 (2018) - Criticality Analysis Process Model
- - NISTIR 8272 (2020) - Impact Analysis Tool for Interdependent Cyber Supply Chain Risks **RESCINDED**
- - NISTIR 8276 (2021) - Key Practices in C-SCRM (Case Studies and Findings)
- - 2nd PD SP 800-161 Revision 1 (October 2021)

EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY

- Critical Software +
- Software Verification +
- Cybersecurity Labeling for Consumers +
- Workshops & Call for Papers
- News & Updates
- Engage
- Fact Sheet
- Resources
- FAQs

Improving the Nation's Cybersecurity: NIST's Response under the Executive Order

Overview:

The President's Executive Order (EO) on "[Improving the Nation's Cybersecurity \(14028\)](#)" issues multiple agencies – including NIST– with enhancing cybersecurity through a variety of initiatives to ensure the integrity of the software supply chain.

Section 4 of the EO directs NIST to solicit input from the private sector, academia, government to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software security. Those guidelines are to include:

- criteria to evaluate software security,
- criteria to evaluate the security practices of the developers and suppliers themselves, and
- innovative tools or methods to demonstrate conformance with secure practices.

The EO calls for NIST to consult with the National Security Agency (NSA), Office of Management and Budget (OMB), and the Department of Justice (DOJ) to ensure that the guidelines are consistent with the

REGISTER | NIST Workshop: EO 14028 - Enhancing Software Supply Chain Security

National Institute of Standards and Technology (NIST) sent this bulletin at 10/26/2021 10:38 AM EDT



Cybersecurity Insights

Registration is now OPEN! Workshop on EO 14028 – Guidelines for Enhancing Software Supply Chain Security Including Standards, Procedures, & Criteria

Join NIST at our upcoming [workshop](#) on November 8, 2021 at 1:00 PM EST as we share and discuss the approach that NIST is taking to support Section 4e of the President's Executive Order (EO) on "[Improving the Nation's Cybersecurity \(14028\)](#)" issued on May 12, 2021. This EO charged multiple agencies – including NIST– with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.

NIST recently released [Draft Special Publication \(SP\) 800-218, Secure Software Development Framework \(SSDF\) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities](#). The SSDF is a set of fundamental, sound practices for secure software development based on established standards and guidelines produced by various organizations. The SSDF directly addresses several practices that were called out in Section 4e—and provides a starting point for discussing other practices that Section 4e

SP 800-161, Revision 1 (2nd Public Draft): Contents

SECTION 1: Introduction

- Purpose
- Target Audience
- Document Use, by Audience Profile
- Background

SECTION 2: Integration of C-SCRM into Enterprise-wide Risk Management



- Business Case
- Multi-Level Org. Roles & Responsibilities
- C-SCRM Program Management

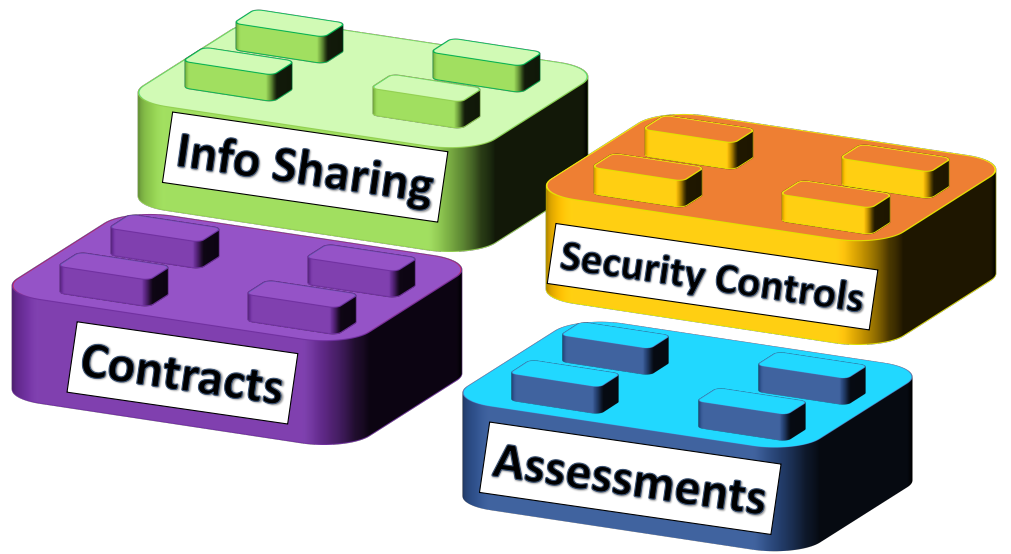
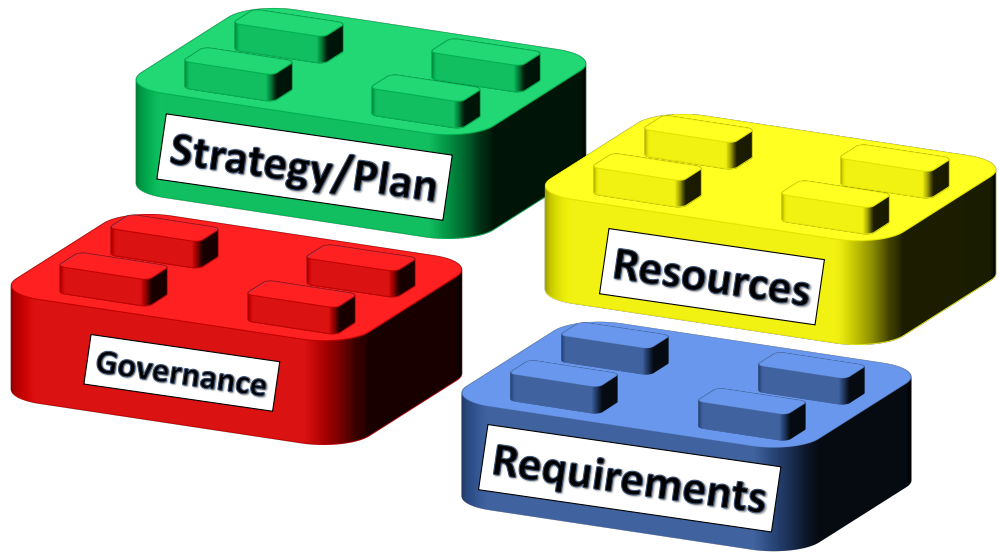
SECTION 3: Critical Success Factors

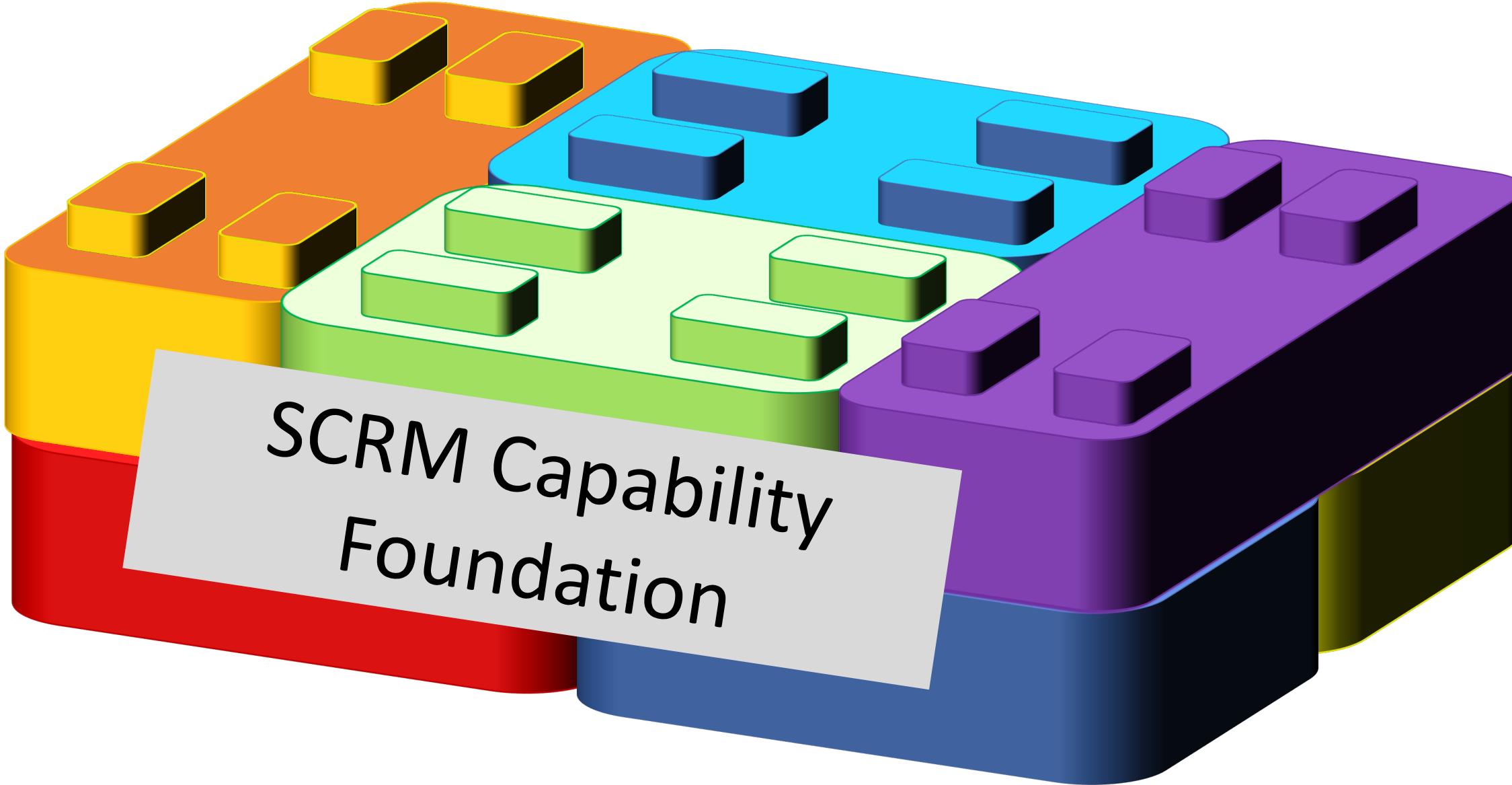
- Acquisition Processes
- Information Sharing
- Training
- Key Practices
- Capability Measurement/C-SCRM Measures
- Dedicated Resources

SP 800-161, Revision 1 (2nd Public Draft): Contents

APPENDICES

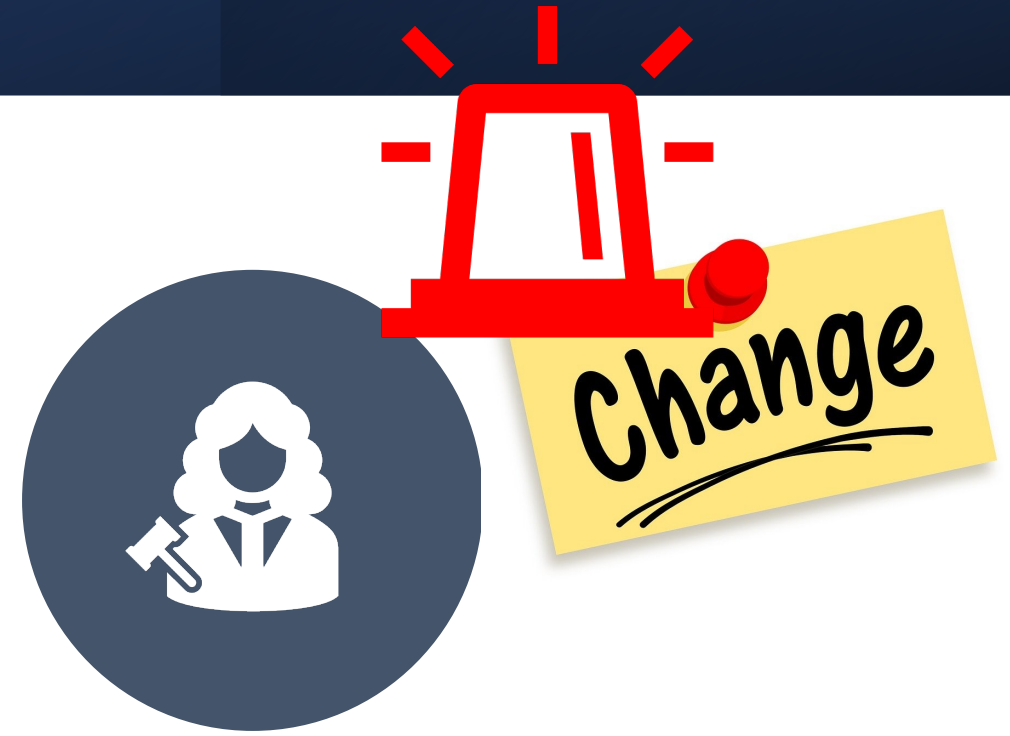
- Appendix A: C-SCRM Controls
- Appendix B: C-SCRM Control Summary Table
- Appendix C: Risk Exposure Framework
- Appendix D : C-SCRM Templates (Strategy & Implementation Plan; Policy; C-SCRM System Plan: Supply Chain Risk Assessment)
- Appendix E: FASCSA. 
- Appendix F: Preliminary Guidelines for Enhancing Software Supply Chain 
- Appendix G: -SCRM Activities in the Risk Management Process
- Appendices H:, I, J : Glossary; Acronyms; References / Methodology



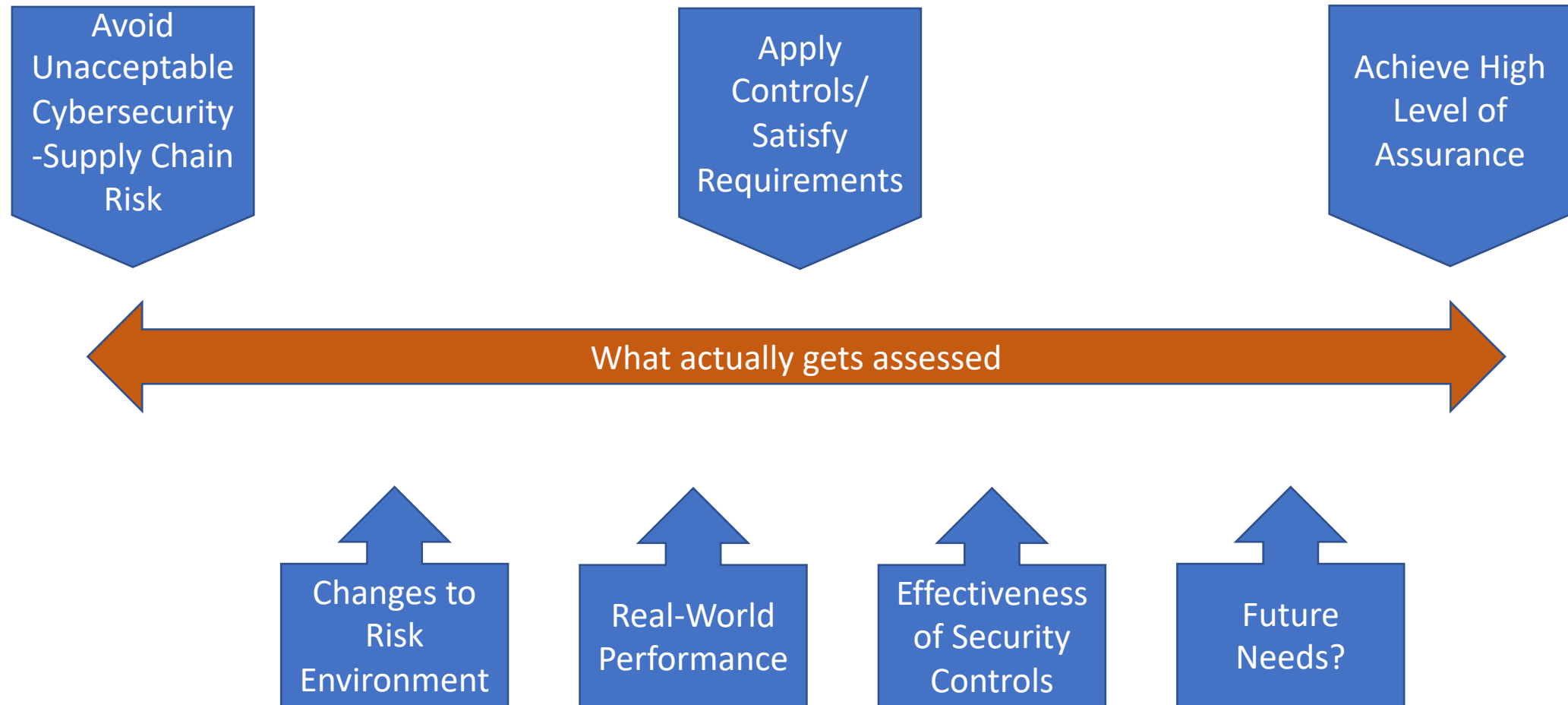


*SCRM Capability
Foundation*

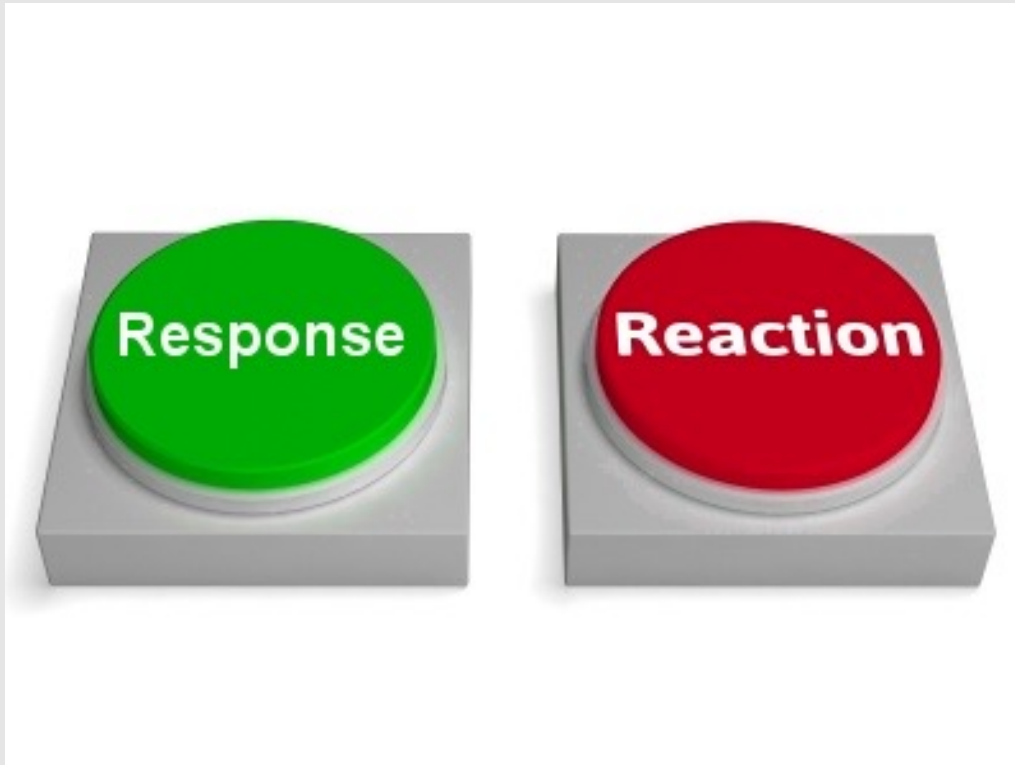
Managing Supply Chain Risk



What is our Assessment Objective?



Prepared or Panicking?



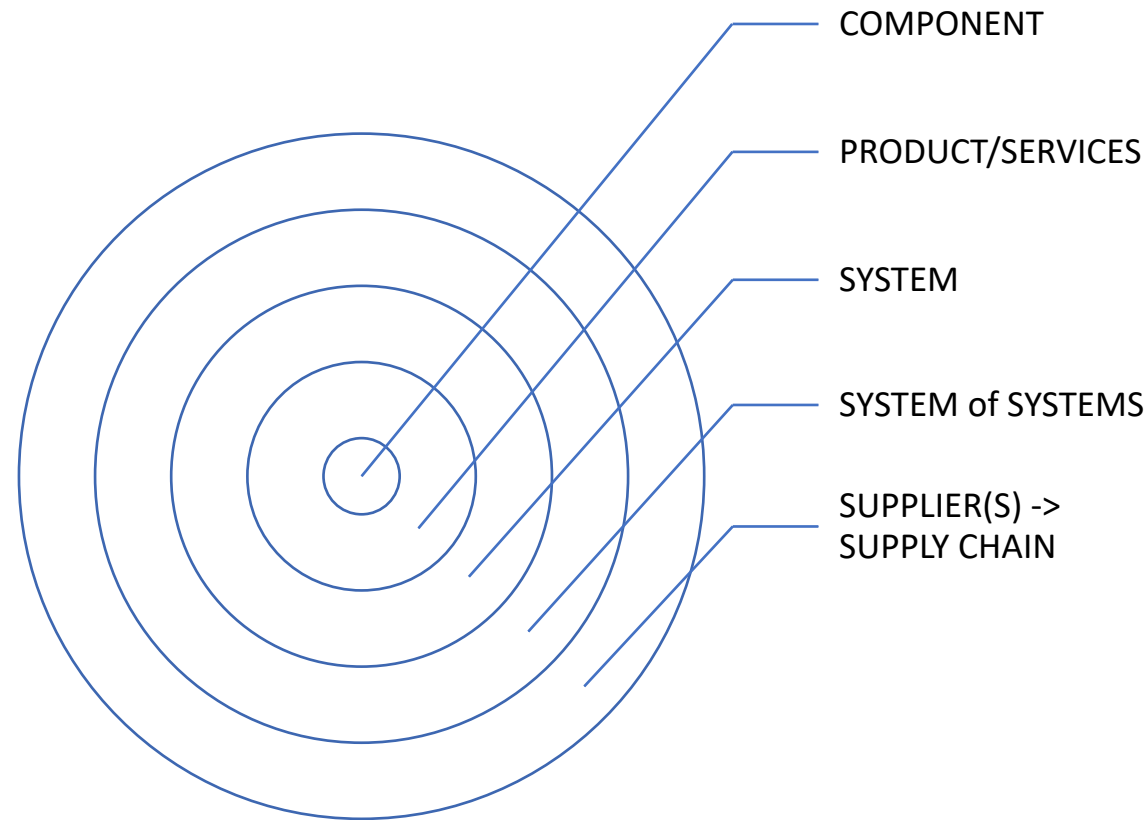
Risk Response Choices:

- Accept
- Transfer
- Mitigate
- Share
- Avoid

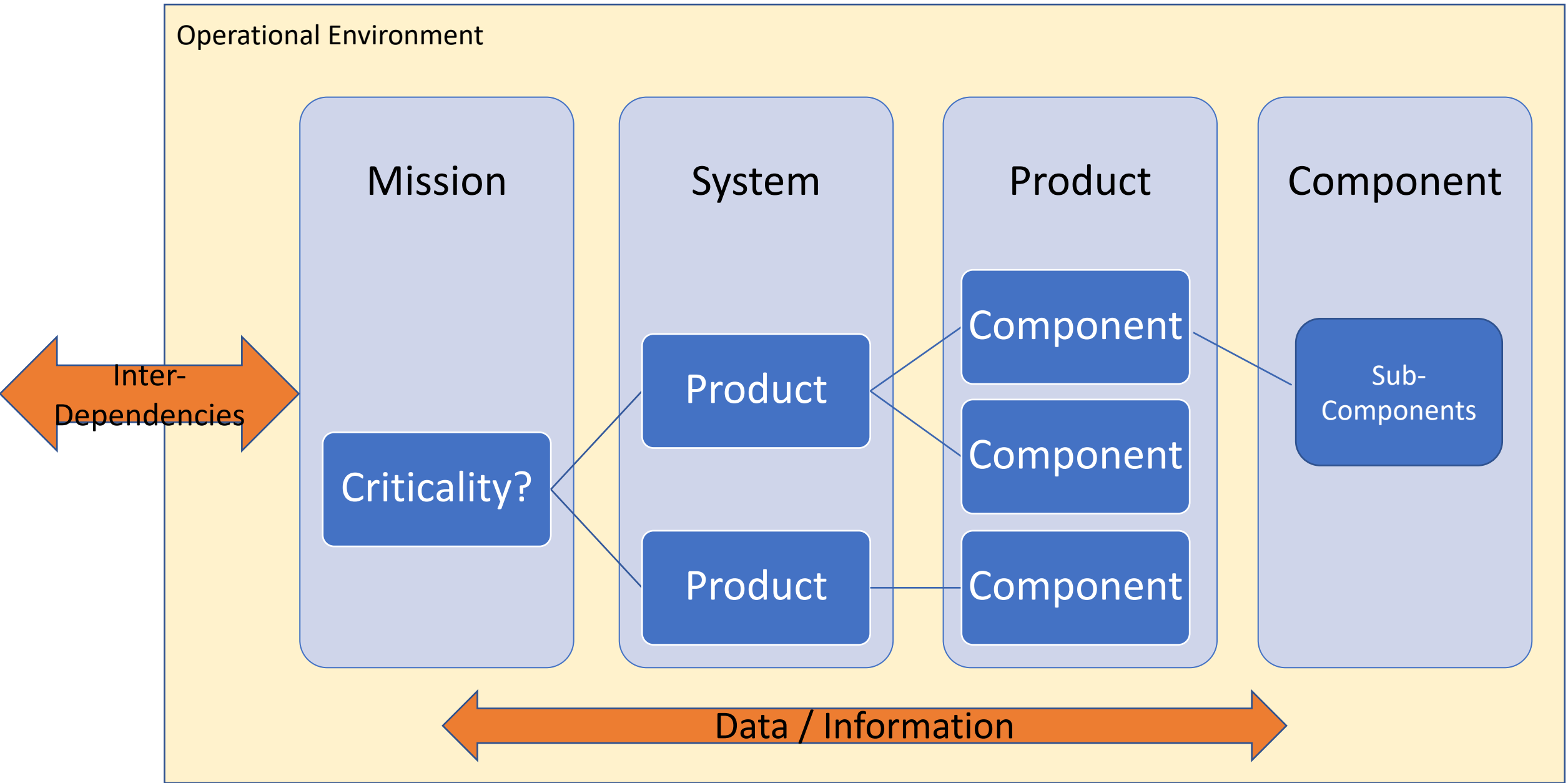
• More Choices:

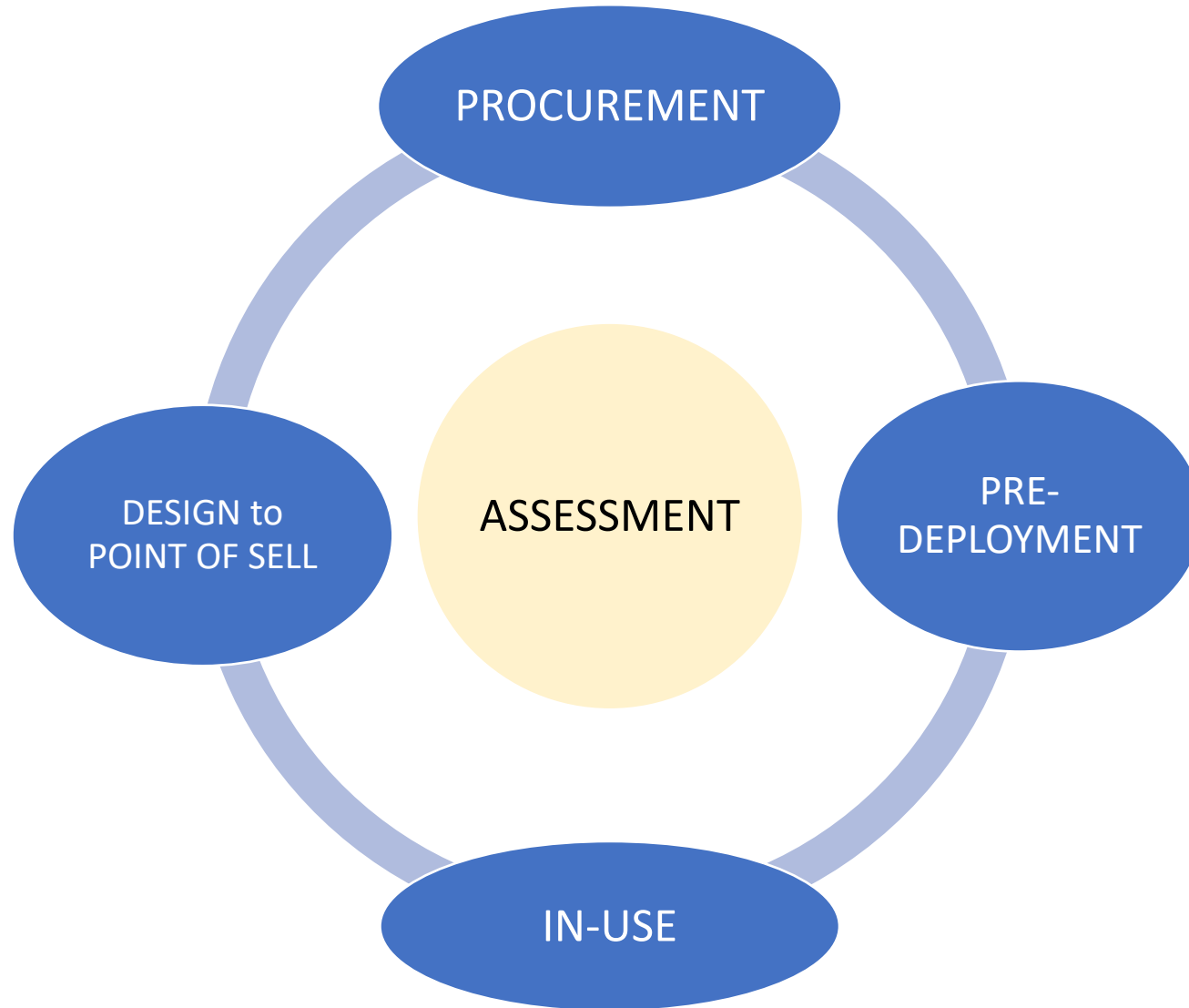
- Ignore (Bad Option but "Real Life")
- Panic!
- Escalate (Get More Help)
- Get More Info
- Report
- Fix

What are we trying to assess? (*now multiply this by “a whole bunch”*)



Purpose & Context Matters





When? Who? Why?
And How Often?

ASSESSING RISK

Research/Examine

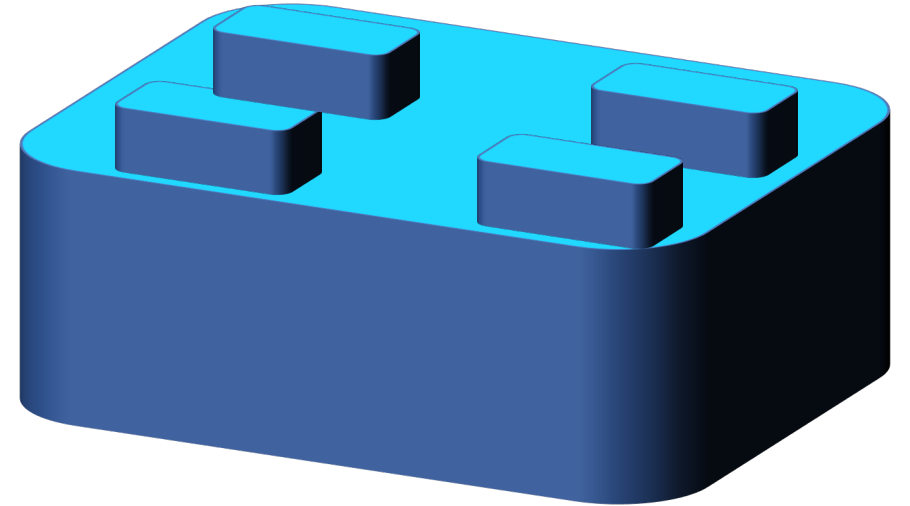
- Data & Information
 - Purpose-specific
 - Risk-relevant
- Category/Weight/Scope

Findings

- Criteria
- Confidence/Quality Level
- Organize/Prioritize/Discard

Conclusions

- Risk Response



Forest

Trees

Big Picture
Perspective/Priorities

Trend Analysis;
Predictive Analytics

Compliance

Find & Avoid What's
Bad

Plug Holes



Federal Acquisition Supply Chain Security Act

- “Government-wide” Framework to Address Supply Chain Risk
- Brings together Agencies with Key Authorities/Expertise into the Federal Acquisition Security Council
- Provides Authority to Exclude/Remove – Sources and Products
- Mandates SCRM for Agencies – Emphasis on Supply Chain Risk Assessments

New “FASCSA Appendix”

- Establishes **Baseline Risk Factors** (Common, Minimal)
- Objectives include:
 - ensuring a level of even treatment of evaluated sources or covered articles;
 - ensuring minimum necessary information is available to the FASC, when required;
 - promoting consistency and comparability across agencies;
 - aiding the conduct of more sophisticated analyses such as trend analysis or causal or correlation relationships between found indicators of risk and realized risks; and
 - having a base of information sufficient to identify and understand potential mitigation options, to inform prioritization or risk response trade-off analysis/decisions, etc.

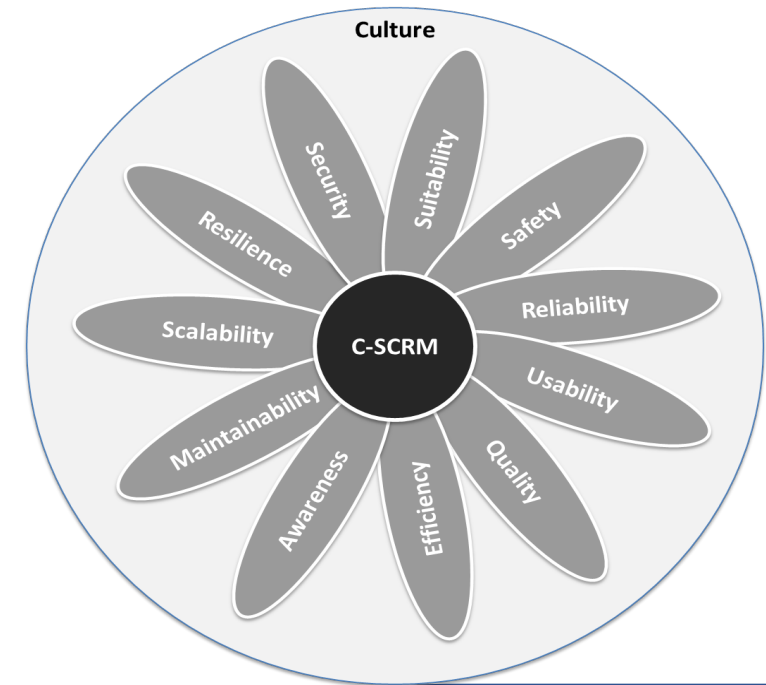
Context (Inherent Risk) Factors

- Criticality
- Information and Data
- Reliance on the covered article or source
- User/operational environment in which the covered article is used or installed, or service performed
- External Agency Interdependencies

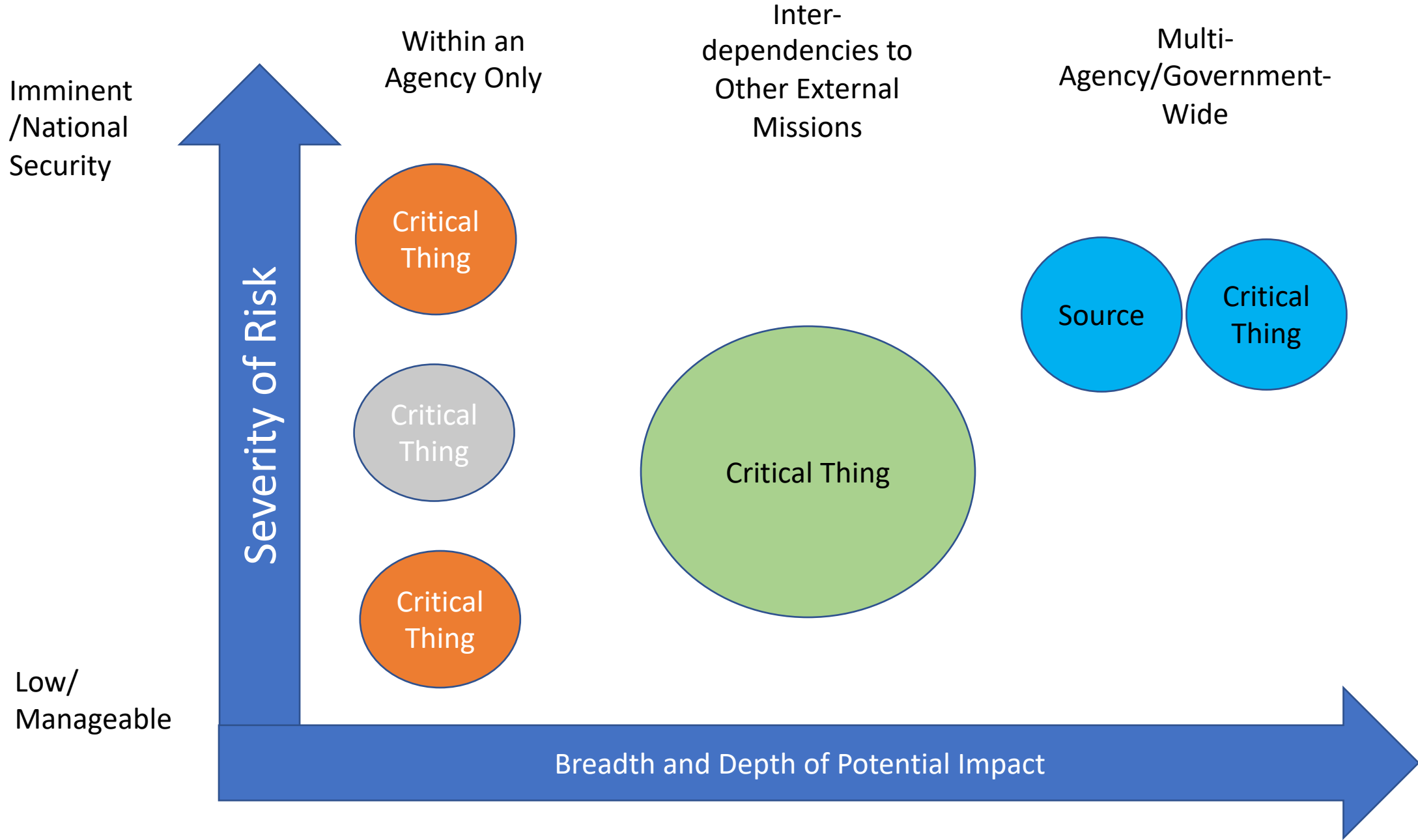
Risk Factors (Inherited from Supply Chain)

- | | |
|--|--|
| • Purpose Functionality, features, and components of the covered article | • Foreign Ownership, Control, Influence (FOCI) |
| • Company Information | • Compliance/Legal |
| • Quality/Past Performance | • Geo-Political |
| • Fraud, Corruption, Sanctions, and Alignment with Government Interest | • *Counterfeit and Non-Conforming Products |
| • Personnel Physical | • Cybersecurity |
| • Physical | • Supply Chain Relationships, Visibility, and Controls |

T	Technically Sound – is it built in a quality manner and meet all the required specifications?	Quality/Performance/Safety
R	Reputation is Solid – what’s the track-record of the product? Are other buyers satisfied?	Multiple Factors
U	Update-able – can components of the product/system be updated if/when needed? How? By whom?	Cybersecurity/Quality/Resilience
S	Secure/Securable – what are the built-in security features? What additional security configurations are possible?	Cybersecurity
T	Tamper-Resistant/Taint-Free – <u>Are</u> shipping and handling methods controlled? Is packaging done in a secure manner? Testing or inspection?	Integrity
W	Warrantied – does the seller or manufacturer stand behind what it is selling?	Quality/Reliability
O	Original – who made it? How do you know?	Counterfeit Avoidance/Quality Assurance/Pedigree
R	Repairable/Replaceable – if it breaks can it be fixed? Can you get a replacement when you need it?	Resilience/Supply Chain Availability
T	Traceable – Do you know who made it? Do you know who touched it before it got to you?	Provenance
H	Hardy – can it withstand the environment it will be in? is it fragile? Does it have built-in redundancy or fail-safe features?	Resiliency
Y	Your Purpose is satisfied - will it do what you need it to do?	Fit-for-Purpose
I	Information – type, amount, sensitivity, inputs/outputs, etc.	Information Assurance/Privacy
N	Network – where will it reside in the network? Is it a closed network? Internet accessible?	Environment/Architecture
C	Connections/Connectability – type of connections? who or what can <u>access, how, how often/long, when, and where</u>	Access
O	Operational Function – what does it do? What shouldn’t it do?	Function/Purpose
N	Necessity – how critical is it? Why is it critical?	Criticality
T	Timeframe – when is it needed? For how long?	Urgency/Duration of Need
E	Exposures – what vulnerabilities does it have?	Vulnerabilities
X	X Factors (Anything else specific to the acquirer’s intended use of the product/system– eg Physical Location, Types of Users, etc.)	Miscellaneous
T	Threats – what are the hazards or threats than can impact its availability or ability to function properly or could compromise the confidentiality, integrity, or availability of information residing within or transiting through the product/system?	Threats



Product/Component Assessment



Assessment Challenges

- Scope: Too much! What to Prioritize? How deep and broad?
- Visibility: Dealing with Known Unknowns and Unknown Unknowns
- Complexity: System of systems; Global supply chains; Embedded Software....Help!
- Info Access/Quality/Confidence: Is my assessment information accurate? relevant? current?
- Capability: Tool, skill and knowledge gaps: Analytic, Technical + SCRM
- Judgment: Conflict of Interest, Bias, GroupThink, “Defensibility”
- People vs Tools: What’s the Right Mix?

Product/Component Assessment Challenges

- Discovery – Who made it? What’s in it? Do I have it in my environment? Can I find it? so I can assess it?
- “White Labeling” – Who REALLY made this?
- Embedded / Integrated Components – Will scanning find all my vulnerabilities?
- Assessment “Artifacts” – What do I need to satisfy my level of required assurance?
 - What can be provided?
 - What can be consumed?
 - What has the most cost-benefit value?

Product Procurement & Pre-Deployment

- Purchases from resellers:
 - Gaps in information about the products, barriers to “flowing down” requirements
- Build in requirements into solicitations
 - One-size fits all or Overly prescriptive language
 - Should a standard be referenced? Which one? And what assurance does that convey?
- “Products” used to perform a service; eg UAVs for aerial inspection
 - Who’s assessing the security of these products?
 - Do these products fall within an agencies’ “authorization boundary”?
- Testing, prior to deployment
 - Who tests? How much? what type? Who assesses results?

How can we better:

- Reuse Assessments and Re-assess the Deltas?
- Discover/Isolate Supply Chain “Critical Paths”
- Establish/Measure “Big Picture” Assessment Effectiveness
- Get/Maintain Info on Interdependencies
- Understand/Keep Current links between: Mission Function-Contractors-Systems-Services
- Define and Report Supply Chain Risk Events or Incidents
- Perform Trend Analysis, Root Cause Analysis, Understand Causal Relationships
- Understand early indicators of potential supply chain risk? patent purchases, M&A activity, etc