Multi-tier Supply Chain Risk Management (SCRM)

Path to Supply Chain Resilience

LOCKHEED MARTIN

Jeff Chang, LM Fellow

Agenda

Key Drivers, DoD SCRM Vision & SCRM Requirements

Illumination/ Multi-tier SCRM Approaches

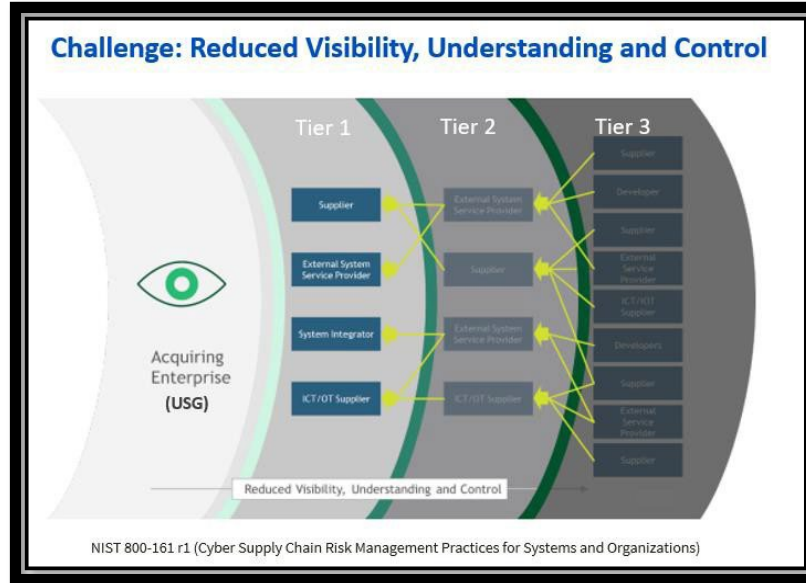Multi-tier SCRM Journey and Lifecycle

Key Takeaways

Q & A

Key Drivers

Securing Defense-Critical Supply Chains

Modernize approach to supply chain resilience — Deliver decisive advantages to our Warfighters in a dynamic threat landscape — Build resilient, competitive, and sustainable supply chains — Collaboration with our allies and partners to build a network of secure global supply chains — Partner with industry to identify and mitigate supply chain issues

Need to Improve Supply Chain Resilience

Securing Defense-Critical Supply Chains — An action plan developed in response to President Biden's Executive Order 14017 — February 2022

Source: Securing Defense-Critical Supply Chains

Challenge: Reduced Visibility, Understanding and Control

Tier 1 — Tier 2 — Tier 3

Acquiring Enterprise (USG)

Reduced Visibility, Understanding and Control

NIST 800-161 r1 (Cyber Supply Chain Risk Management Practices for Systems and Organizations)

Source: NIST 800-161 r1

SCRM Plan (DI-MGMT-82256)

Supply Chain Risk Identification (shall include in detail):
- Intelligence-based and counter-intelligence-based techniques and commercial business tradecrafts employed to **uncover and map supplier networks**
- Risk categories – Product/quality, financial, political and regulatory, foreign influence, operational, environment, technology and human capital

Supply Chain Analysis / Assessments (shall include):
- Process to scan the contractor's **full-spectrum supply chain network**, applying customizable risk lenses, to assess supply chain risks that could impact the Government's program

Other Drivers

Geopolitical Tensions	REE/Specialty Metal Sourcing Restrictions	Chip Shortages
COVID-19 Pandemic	Decoupling from China	Provenance Tracking

Growing Demand for Supply Chain Resilience and Multi-tier SCRM

National Defense Industrial Strategy

National Defense Industrial Strategy
DEPARTMENT OF DEFENSE
2023
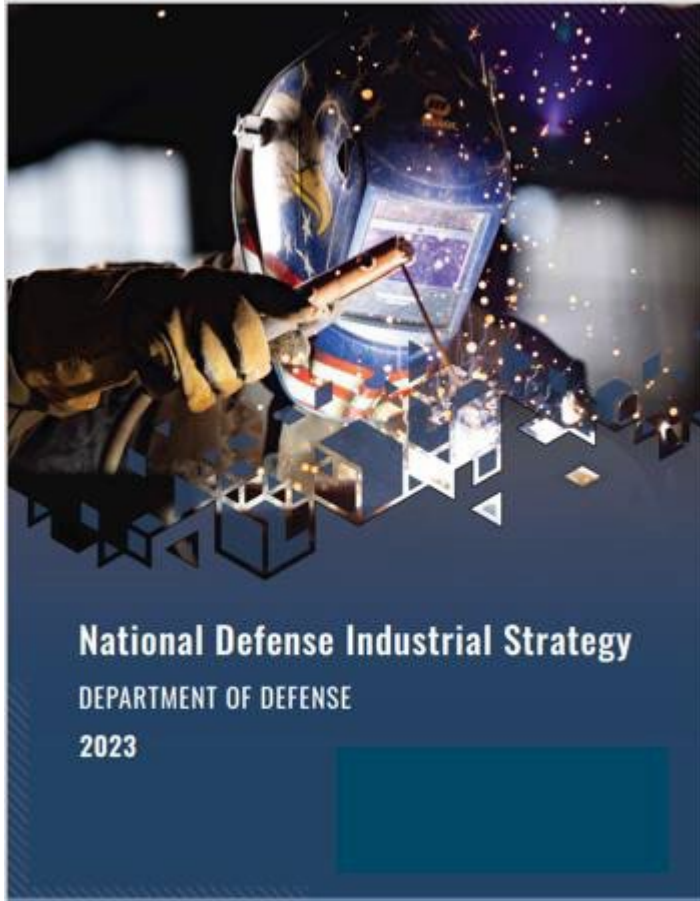
- "A robust and resilient industrial base provides the enduring foundation for military advantage."

- The NDIS lays out four long-term priorities:
    - Resilient Supply Chains
    - Workforce Readiness
    - Flexible Acquisition
    - Economic Deterrence

- Ensuring the health of sub-tier suppliers is crucial to a healthy, diverse, and modernized DIB.

- Currently, the health of sub-tier suppliers, manufacturing capacity, and lack of visibility into our critical supply chains create unique challenges
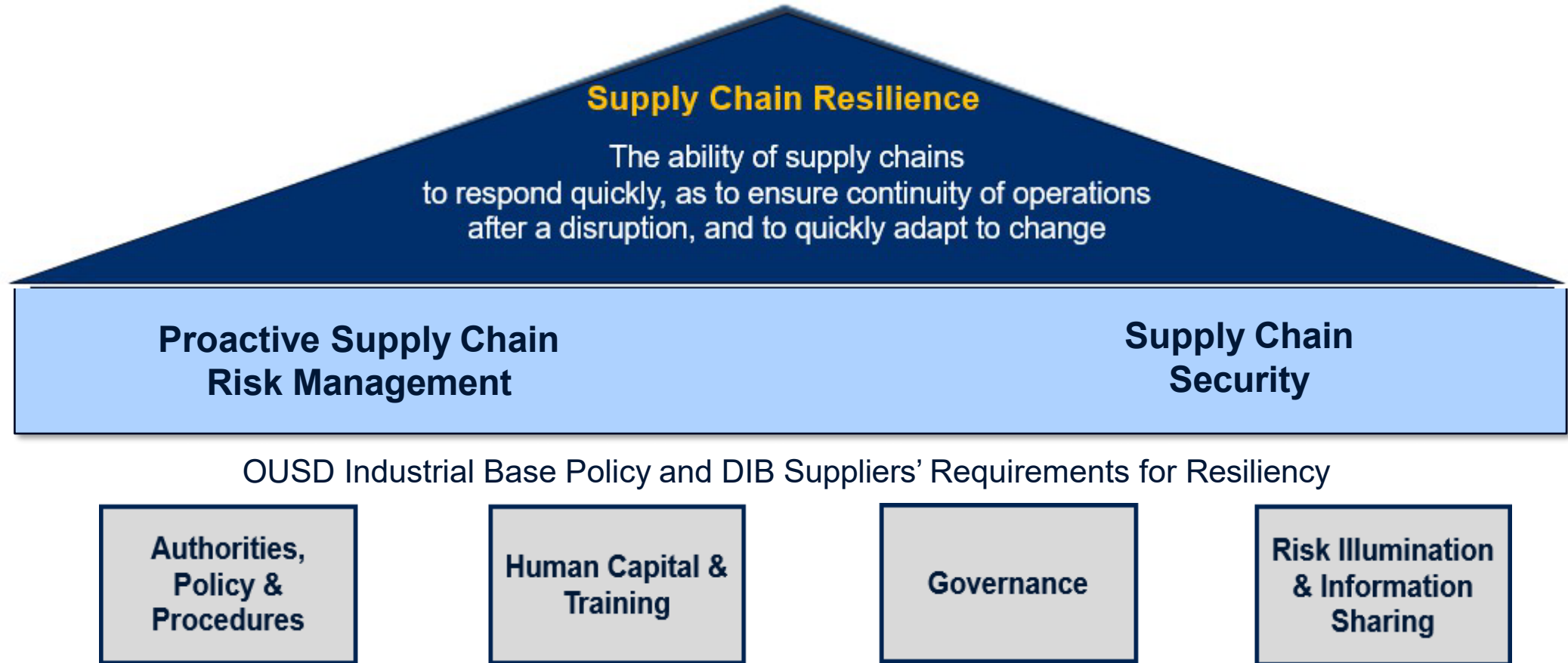
FY24 NDAA – Pilot Program (Section 856)

- DoD shall establish a pilot program "to analyze, map, and monitor supply chains for up to five covered weapons platforms"

- DoD may use a combination of commercial tools and tools available to the Department of Defense to carry out the program

- Identify impediments to production and opportunities to expand the production of components of such a covered weapons platform

- Identify critical suppliers for such covered weapons platforms

Upcoming Regulations

- DFARS 2023-D003. Contractors must disclose provenance of all rare earth magnets

    o   Where rare earth elements mined;

    o   Where refined into oxides

    o   Where made into metals and alloy

    o   Where magnet sintered or bonded and magnetized

- Goes into effect no earlier than June 2025 and after SecDef certifies there is a process to ensure collected information does not present security risk

- Based on section 857, FY23 NDAA

DoD SCRM Vision

Delivering Integrated Deterrence requires a holistic, coordinated, cohesive approach to Supply Chain Risk Management (SCRM) that will strengthen the resiliency of our defense supply chain

Supply Chain Resilience

The ability of supply chains
to respond quickly, as to ensure continuity of operations
after a disruption, and to quickly adapt to change

Proactive Supply Chain Risk Management

Supply Chain Security

OUSD Industrial Base Policy and DIB Suppliers' Requirements for Resiliency

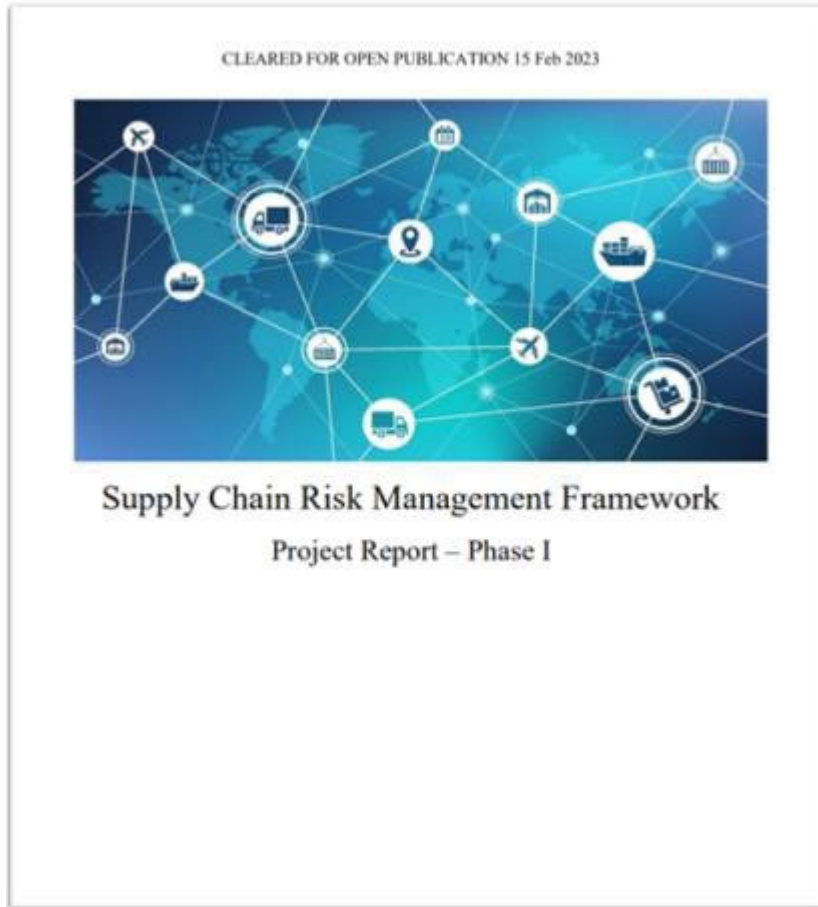| Authorities, Policy & Procedures	Human Capital & Training	Governance	Risk Illumination & Information Sharing

* - For OUSD(A&S) Industrial Base Policy & DIB suppliers

Source: DoD SCRM Framework (Feb 2023)

Supply Chain Resilience Is The Outcome of Proactive SCRM and Supply Chain Security

LOCKHEED MARTIN

LOCKHEED MARTIN

DoD SCRM Framework

CLEARED FOR OPEN PUBLICATION 15 Feb 2023

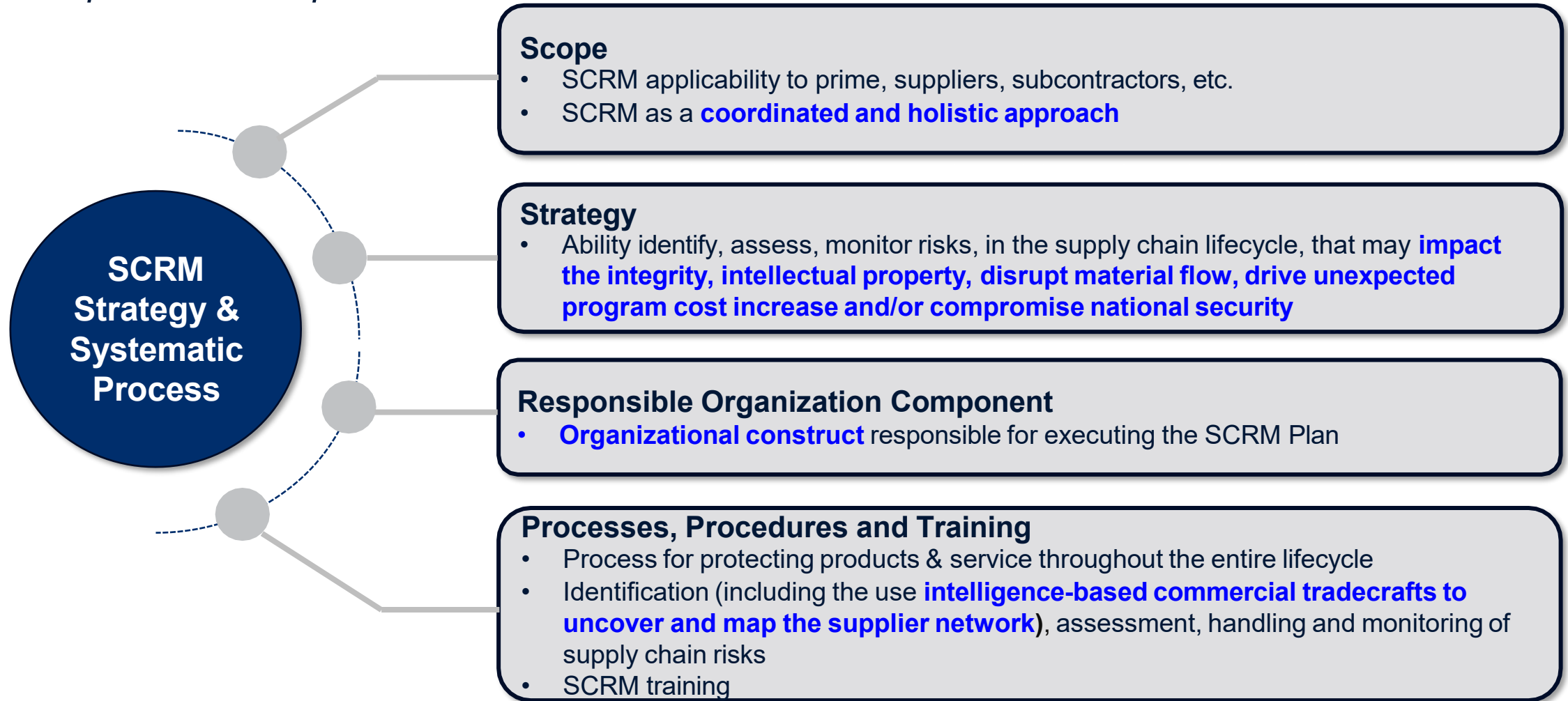Supply Chain Risk Management Framework
Project Report – Phase I

- Multiple Organizations with DoD address Supply Chain risks

- Various supply chain risks:

  - Single and sole source parts

  - Counterfeit items

  - Diminishing Manufacturing Sources & Material Shortages (DMSMS)

  - Obsolescence

  - Supply chain disruptions

  - Cyber vulnerabilities

  - Foreign sourced parts from within or associated with potentially adversarial nations

- ASD(Sustainment) developed and published common SCRM framework and taxonomy

SCRM Plan (DI-MGMT-82256A)* Summary

Systematic process used to identify, assess, handle & monitor supply chain risks associated with the product to be provided

SCRM Strategy & Systematic Process

Scope
- SCRM applicability to prime, suppliers, subcontractors, etc.
- SCRM as a **coordinated and holistic approach**

Strategy
- Ability identify, assess, monitor risks, in the supply chain lifecycle, that may **impact the integrity, intellectual property, disrupt material flow, drive unexpected program cost increase and/or compromise national security**

Responsible Organization Component
- **Organizational construct** responsible for executing the SCRM Plan

Processes, Procedures and Training
- Process for protecting products & service throughout the entire lifecycle
- Identification (including the use **intelligence-based commercial tradecrafts to uncover and map the supplier network**), assessment, handling and monitoring of supply chain risks
- SCRM training

* Related requirements: DI-MGMT-82255A, DI-MGMT-82147A, DI-MGMT-82147A

Source: Office of Security of Def

LOCKHEED MARTIN

Supply Chain Mapping & Risk Monitoring Approaches

1

Mapping Buyer-Seller Relationships
- Leveraging structured and unstructured federated data sources, e.g., bills of lading
- Perform Due Diligence and monitor all potential supplier site risks

2

Mapping Discrete Item / BOM Relationships
- Building out an item's actual multi-tier BOM with supplier validations
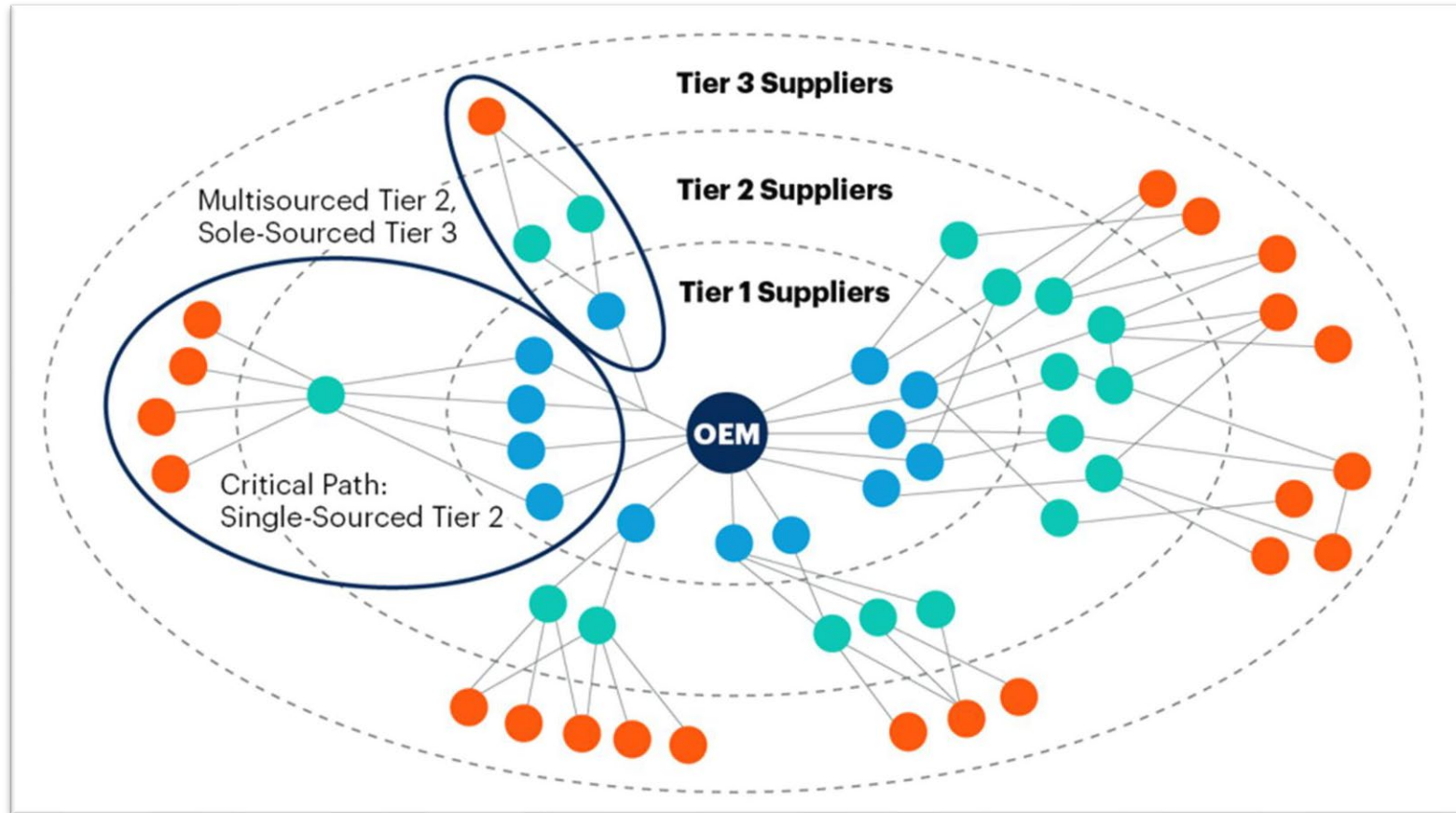- Monitor actual supplier site and product risks

3

Combination of 1 & 2 above
- Map an item's actual multi-tier BOM
- Perform Due Diligence & monitor relevant supplier site and product risks

Supplier Network Visibility

Mapping Critical Component's multi-tier supplier network

Source: Gartner

Viewing the Supply Chain as A Complex Supply Chain Ecosystem

Key Aspect of Multi-tier SCRM

Visibility of Supply Chain Network
- Gaining visibility multi-tier supply chain to understand dependencies, vulnerabilities, and potential points of failure

Data Enrichment & Risk Assessment
- Assessing risks across the entire supply chain; including identifying various types of risks and evaluating their potential impact on the organization

Transparency & Collaboration
- Collaborating and communicating with partners across multiple tiers of the supply chain; including sharing risk information, coordinating risk mitigation efforts, and developing risk response plans

Risk Response/ Resilience Planning
- Establishing resilience within the supply chain to withstand and recover from disruptions. May involve diversifying supplier sources, developing alternate supply chain routes, etc.

Continuous Monitoring
- Monitoring of risks to mitigate risks as the supply chain landscape evolves.; including leveraging technology, such as real-time tracking and analytics, to detect and respond to emerging risks

Path to Supply Chain Visibility & Resilience

1
- Obtain Technical Data Package (CAD drawing, Parts Lists, First Article of Inspection, etc.) from Prime or Tier 1 supplier

2
- Transform technical data into clean, structured indented BOMs (mapping the supply chain network)

3
- Invite N-tier suppliers to validate BOM and provide additional data (lead times, M/B relationships, current prices/ sources, Yields, etc.
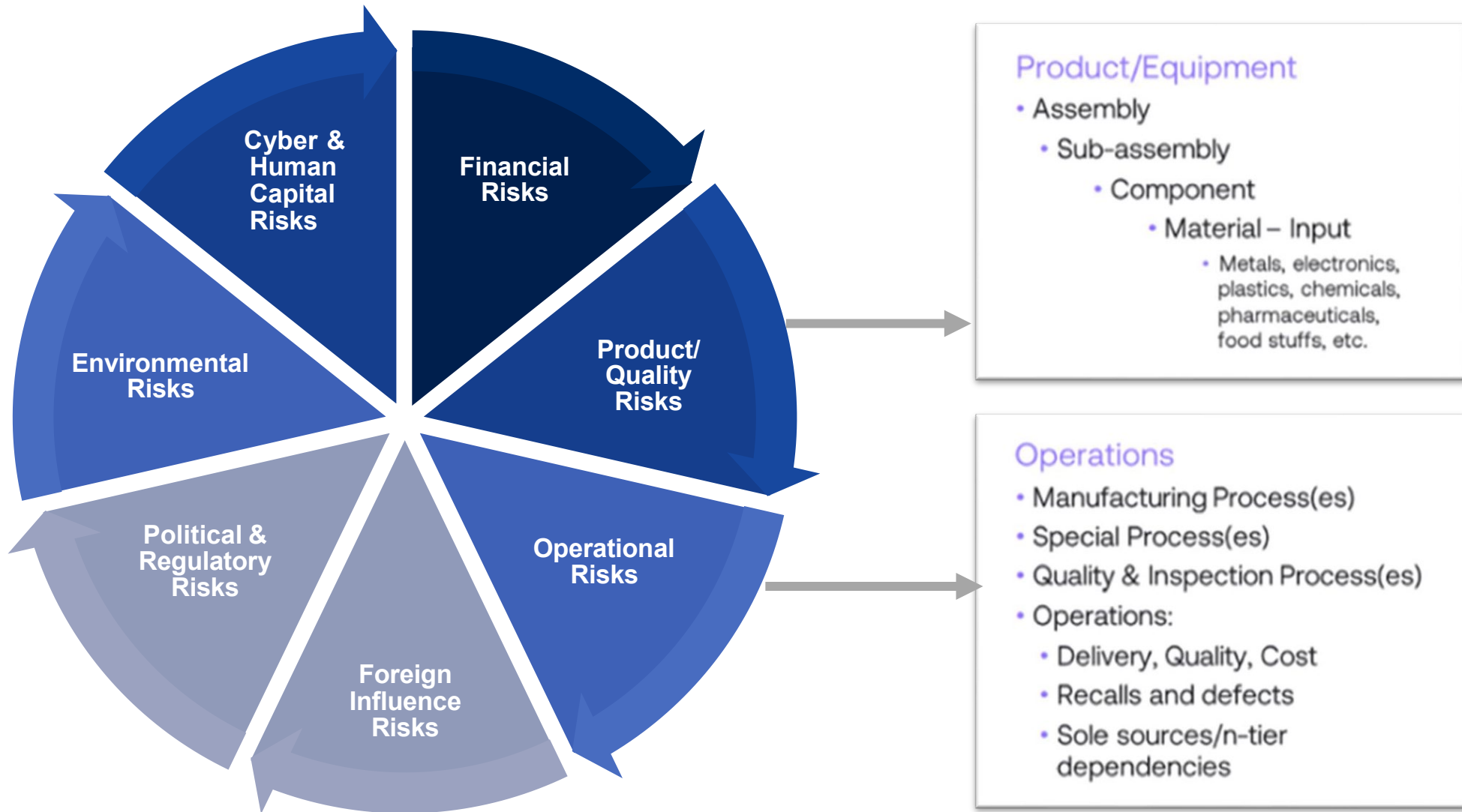
4
- Enrich supplier risk data (risk profiles and continuous risk monitoring)
- Identify alternative parts/materials and entity risks
- Validate & take proactive risk mitigation actions

5
- Disclosure risk when required
- Track validated risks to closure

May Consider Demand Aggregation & Procurement Optimization Next

DI-MGMT-82256 SCRM Risk Categories

Product/Equipment
- Assembly
  - Sub-assembly
    - Component
      - Material – Input
        - Metals, electronics, plastics, chemicals, pharmaceuticals, food stuffs, etc.

Operations
- Manufacturing Process(es)
- Special Process(es)
- Quality & Inspection Process(es)
- Operations:
  - Delivery, Quality, Cost
  - Recalls and defects
  - Sole sources/n-tier dependencies

Wheel labels: Financial Risks, Product/Quality Risks, Operational Risks, Foreign Influence Risks, Political & Regulatory Risks, Environmental Risks, Cyber & Human Capital Risks
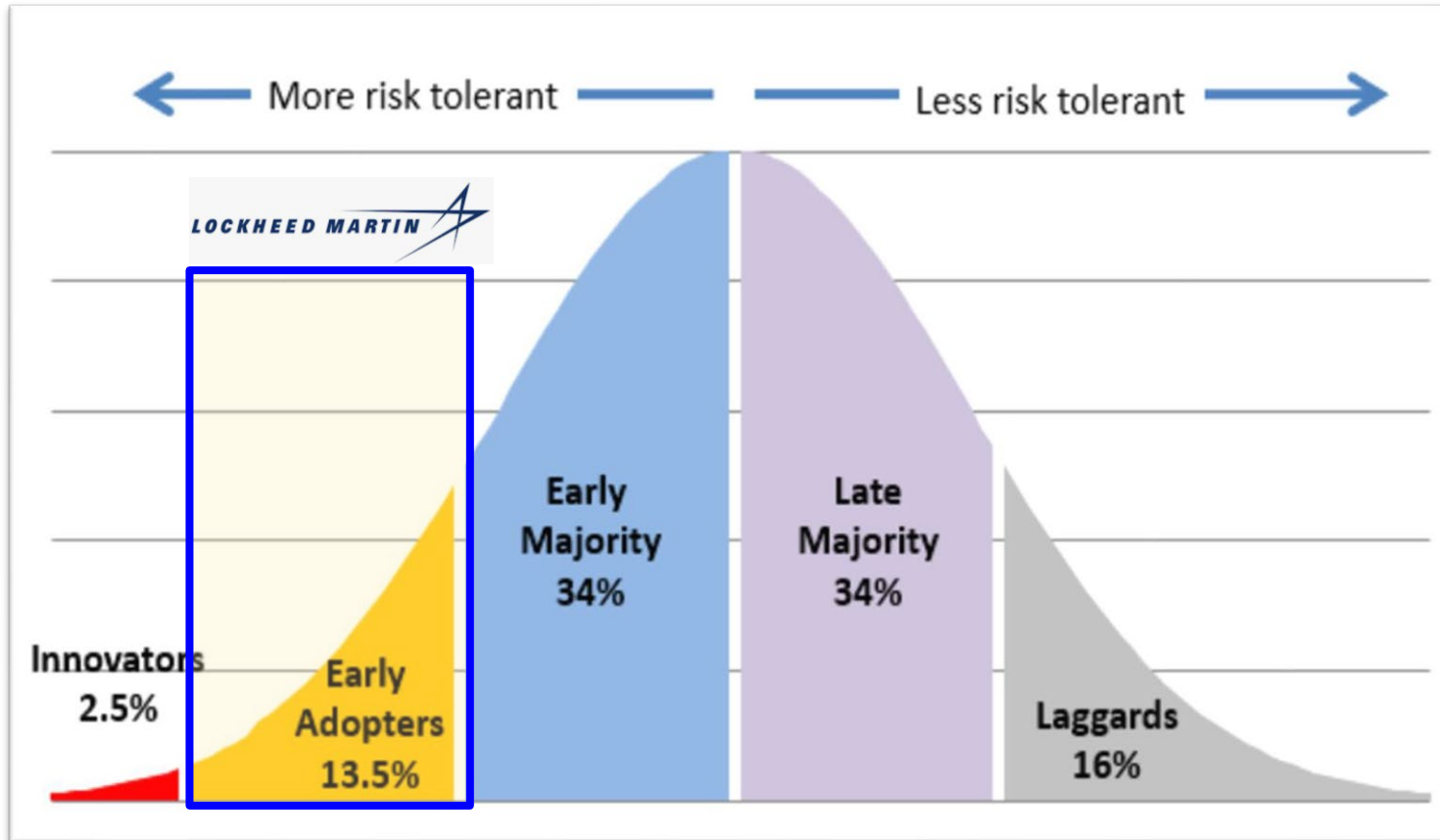
Source: DI-MGMT-82256

Notional Indented BOM w/ Part Risk Information

Risk Indicator

Tier 1 Supplier assembly ✓

Tier 2 Sub-assembly ✓

Tier 3 Component ✓

Tier 4 Material Input ✓

Tier 2 Sub-assembly !

Tier 3 Component ✓

Tier 3 Component ✓

Tier 3 Component ✓

Part Risk Information ✕

Risk | Inventory | Price

Overall Risk	78%	Estimated Years to EOL	0.0
Lifecycle Risk	High	Crosses Available in Part Category	Yes
Multi-Source Risk	Low	Other Sources	15
Inventory Risk	High	Reach Compliant	No
RoHS Risk	High	RoHS Compliant	Yes
		Counterfeit Risk	75%
Time Since Introduction (years)	12	Conflict Minerals	DRC Conflict Free(Undeterminable for specific parts)
Lifecycle Stage	Obsolete	Rare Earth Element Info	
Part Status	Obsolete	Lead Free	No
Estimated Years to EOL	0.0	Countries of Origin	China

Source: 3rd party vendor (Used with Permission)

Distribution Statement A. Distribution Unlimited.

SCRM Journey
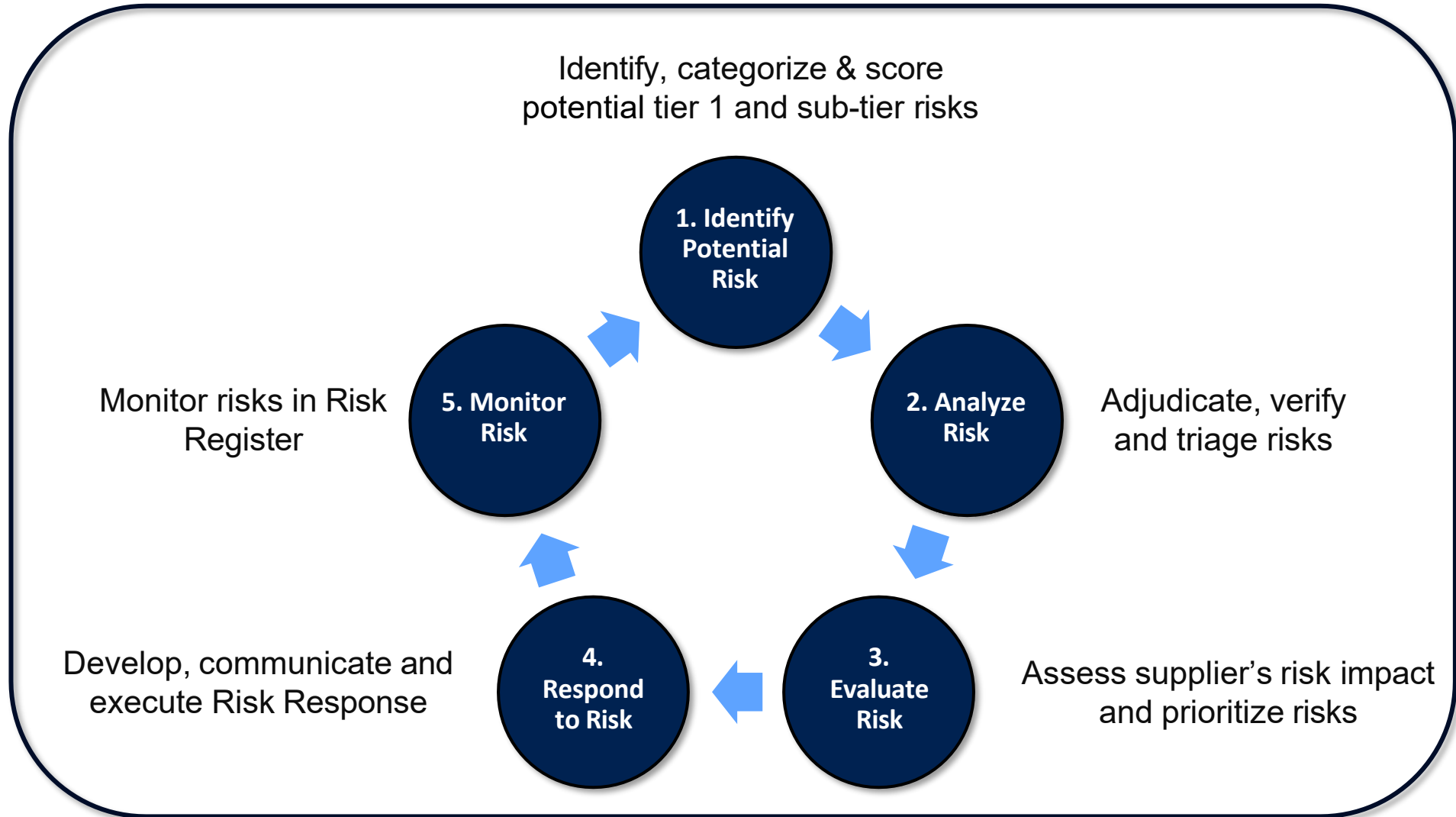## *Illumination/ Multi-tier SCRM Technology Adoption Curve*

Source: Wikipedia

Potential Milestones

- ID functional/ technical requirements
- Conduct Market Research
- Select 3rd party vendor for internal pilots
- Conduct pilots & down select
- Issue contract to selected tech vendor
- Technology solution/ tool validation
- Establish SCRM organization & processes
- Develop & execute SCRM plan
- SCRM Center of Excellence (COE)

Supply Chain Risk Management Lifecycle

Identify, categorize & score
potential tier 1 and sub-tier risks

1. Identify Potential Risk

Adjudicate, verify
and triage risks

2. Analyze Risk

Assess supplier's risk impact
and prioritize risks

3. Evaluate Risk

Develop, communicate and
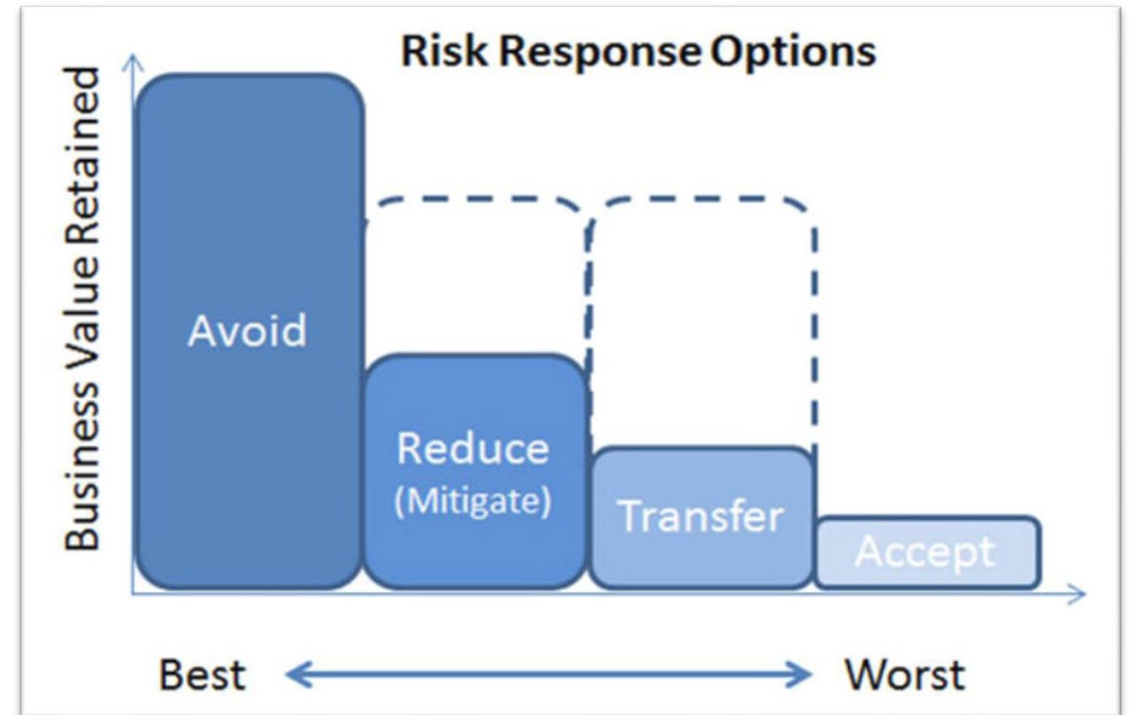execute Risk Response

4. Respond to Risk

Monitor risks in Risk
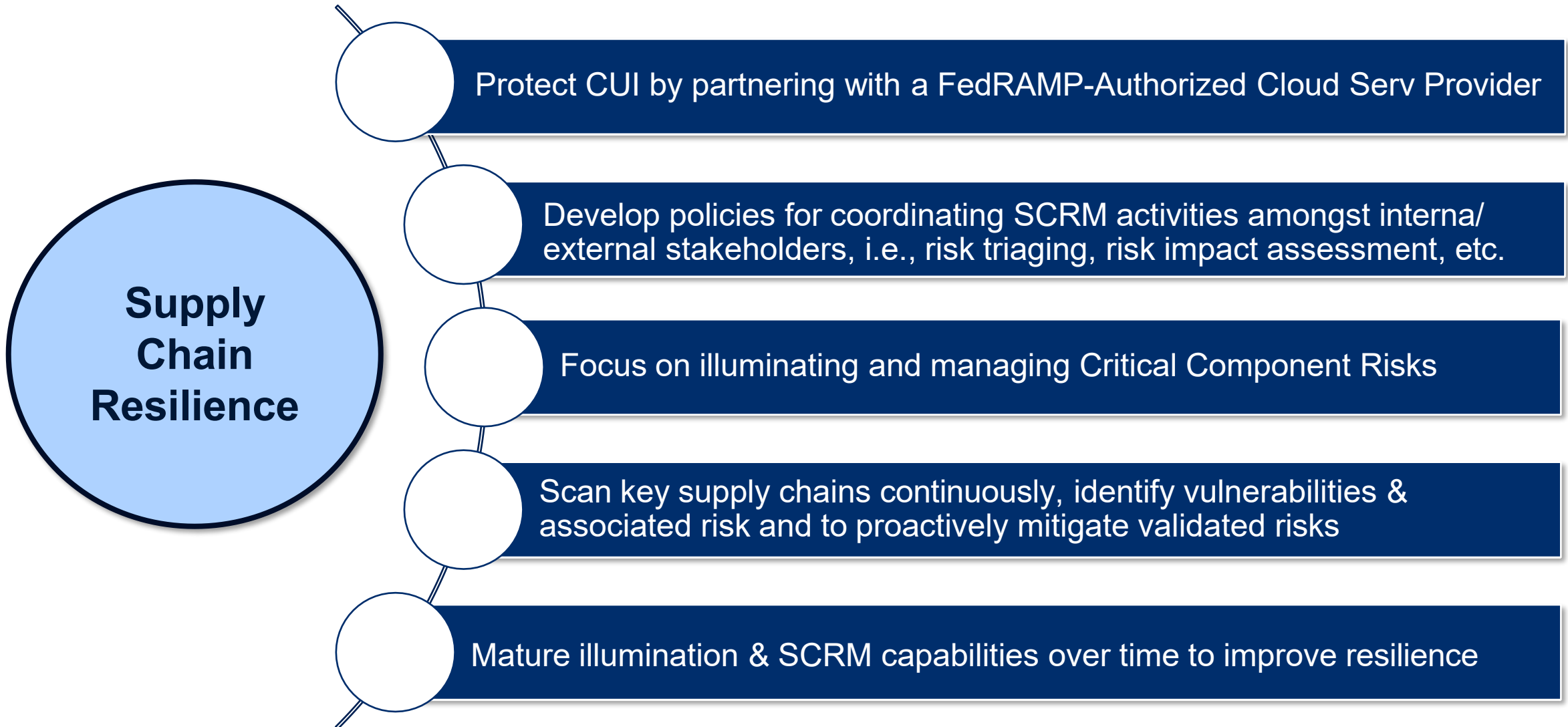Register

5. Monitor Risk

Risk Response Options

- Risk Response Planning is a process of identifying what you will do with all the risks in your profile.

- 4 main response options:

Key Takeaways

Supply Chain Resilience

- Protect CUI by partnering with a FedRAMP-Authorized Cloud Serv Provider

- Develop policies for coordinating SCRM activities amongst interna/ external stakeholders, i.e., risk triaging, risk impact assessment, etc.

- Focus on illuminating and managing Critical Component Risks

- Scan key supply chains continuously, identify vulnerabilities & associated risk and to proactively mitigate validated risks

- Mature illumination & SCRM capabilities over time to improve resilience

Q & A

LOCKHEED MARTIN

LOCKHEED MARTIN