DoD Supply Chain Risk Management Guidebook

Roles, Best Practices, and Strategies

Contents

Foreword

The Department of Defense (DoD) operates within a vast global framework, utilizing national and international supply chains to develop and maintain critical weapon systems, products, and services. Ensuring the security and resiliency of these supply chains is crucial for preserving the operational effectiveness and freedom of our forces. By protecting against disruptions and vulnerabilities, especially those from adversarial nations, we can maintain the strength and effectiveness of our military.

The supply chain risk management (SCRM) process often begins during the development of science and technology (S&T) and can start as early as the requirements phase before a formal acquisition program. This guidebook emphasizes the importance of SCRM in the acquisition program office, led by systems engineers who collaborate with S&T managers, product support managers, and logisticians. The goal is to establish an initial supply chain that ensures immediate operational effectiveness and sustainment for each system. Early emphasis on SCRM allows for thorough evaluation and strengthening of design and supply chain considerations.

Program managers (PMs) are responsible for establishing formal risk management processes that prioritize and mitigate programmatic risks within constraints. PMs must have a comprehensive understanding of their supply chains and identify potential risks. In a dynamic and contentious environment, the ability to quickly establish industrial capabilities to produce essential items for weapon systems readiness is often limited, highlighting the need for proactive risk management.

This guidebook provides an overview of recommended roles, best practices, and strategies for managing supply chain risk, aligning with the existing program risk management framework outlined in the DoD Risk, Issue, and Opportunity Management Guide. Over the next two years, we plan to refine and enhance this guidebook and the accompanying SCRM Mitigation Library, incorporating examples and lessons learned from program offices and supply chain activities to increase its value.

Stephanie Q. Howard, Brigadier General, USA
Performing the Duties of Deputy Assistant Secretary of Defense for Logistics
Office of the Undersecretary of Defense, Acquisition and Sustainment
June 2025

Record of Changes

DoD Supply Chain Risk Management Guidebook Version 1.0.

Approved by:

BG Stephanie Q Howard Digitally signed by BG Stephanie Q Howard Date: 2025.06.09 13:24:05 -04'00'

Signature:

9 June 2025

Date:

For questions concerning this guidebook, please consult with your Component and Agency SCRM functional office. Recommendations for updates and feedback to this guidebook may be sent to:

The Office of the Assistant Secretary of Defense (Sustainment)
ATTN: Supply Chain Risk Management Integration Center
3500 Defense Pentagon
Washington, DC 20301-3500

Or at the link below.

Click here: Link

1.0 Introduction – DoD SCRM Ecosystem

Supply chain risks are not unique to the Department, but such risks take on greater urgency when considered in the light of national security. Figure 1.0, *Example Supply Chain Risks to Weapon Systems* illustrates some of the risks that DoD faces in keeping weapon systems operational. Each example risk below, on its own, can prevent full operational capability negatively impacting readiness.

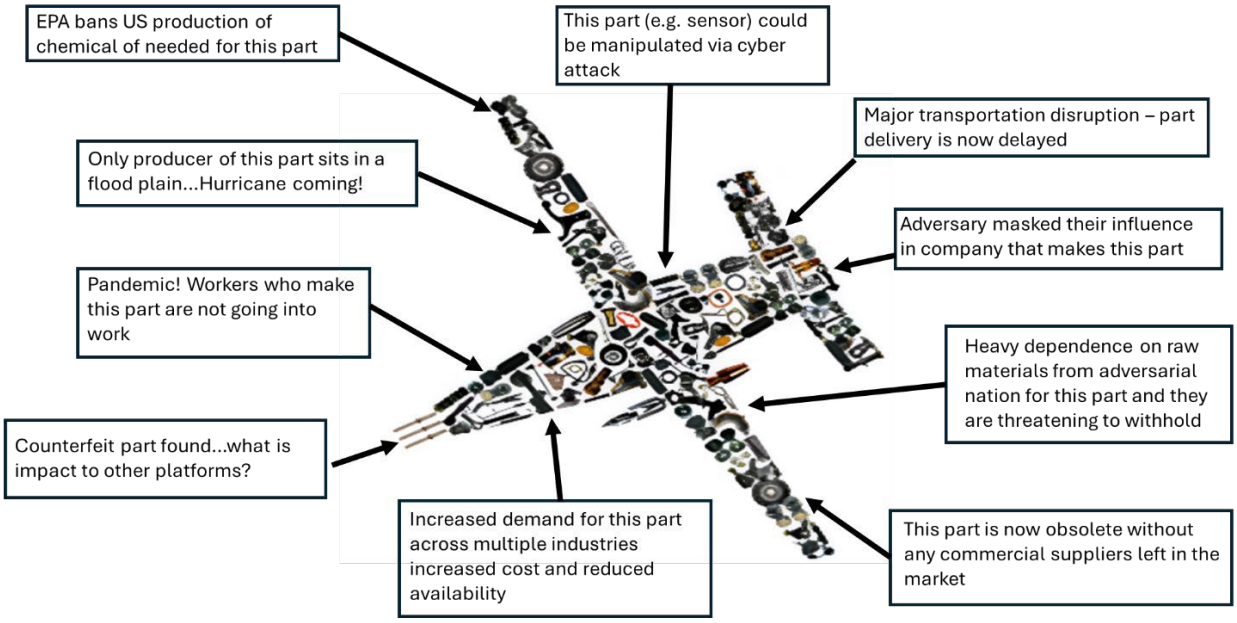

Figure 1.0. Example Supply Chain Risks to Weapon Systems

DoD's ability to effectively manage each of these risks requires an ecosystem of diverse organizations and professionals, many of which typically may not work directly with each other, highlighting the importance for a PM to take a holistic and broad view of risks and skill sets needed for their respective systems.

2.0 Roles & Scope

2.1. Roles

A PM, in collaboration with industry partners, plays a crucial role in integrating supply chain risk into the overall risk management practices throughout the life cycle of a system or capability. The role includes related activities, such as capabilities-based assessment, information communication technology (ICT) and program protection, materiel management, and cyber-supply chain risk management (C-SCRM). A PM's key responsibilities include:

- *Risk Identification and Analysis*: The PM follows the DoD *Risk, Issue, and Opportunity Management Guide* (*RIO Management Guide*) to manage risks, including those in the supply chain. The process identifies and analyzes risks related to:
    - diminishing manufacturing sources and material shortages (DMSMS)
    - obsolescence

- parts management
- cybersecurity
- counterfeit components
- reliability
- producibility
- environmental factors and
- transportation.

By collaborating with the intelligence community and industry partners, PMs identify potential threats to the supply chain, such as supplier reliability, geopolitical issues, and cybersecurity. Integrating this threat information into the risk management plan allows PMs to prioritize vulnerability management and better assess risk likelihood. Following the RIO Management Guide and NIST guidelines (SP 800-161r1 and 800-30), PMs evaluate and prioritize the likelihood and consequences of these risks to develop effective mitigation strategies. Once risks are identified, PMs collaborate with stakeholders to develop countermeasures and mitigation strategies. These stakeholders include:

- legal
- contracts
- counterintelligence
- industry partners
- Industrial Base Analysts
- engineers [system security or lead]
- program protection [lead or specialists]
- logistics
- product support
- security management
- information protection
- acquisition intelligence
- software
- test engineers

Risk mitigation includes four options: 1. *accept*, 2. *avoid*, 3. *transfer*, or 4. *Control*. Control strategies often involve diversifying suppliers, enhancing cybersecurity measures, incorporating appropriate Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) provisions and clauses into the relevant contract, and establishing continuity of operations plans.

- *Prioritize Risks*: The program office should prioritize risk to address the highest risks first. Because of limited resources and time, developing and implementing strategies or plans for all potential threats and vulnerabilities in the supply chain may not be possible.
- *Identify Contract Requirements*: While only the legal advisor can conduct a legal sufficiency review, the PM, along with the contracting officer and the legal advisor, reviews the contractual action for legal sufficiency, which includes reviewing that the FAR and DFARS provisions, clauses and statutory compliance are included in contracts to help mitigate supply chain risks (e.g., avoid or control). In addition, the PM works with other stakeholders to include contract requirements and deliverables from industry partners to increase visibility of supply chain fragility, DMSMS/obsolescence, software supply chain, cybersecurity supply chain restrictions, and vendor exclusions and other potential

risks. The contract requirements and deliverables must be included in the contract. These requirements will vary in scope depending on the level of effort and priority focus areas.

- *Stakeholder Collaboration*: The PM fosters collaboration between different departments, such as engineering, product support, program protection, counterintelligence, and contracting; and the legal advisor reviews for legal sufficiency.
- *Training and Awareness*: The PM identifies training opportunities and Defense Acquisition Workforce Improvement Act (DAWIA) certification guidelines and raises awareness to educate employees about supply chain risks and the importance of following risk management protocols.
- *Monitoring and Reporting*: The PM, along with industry and sustainment partners, continuously monitors the supply chain using government and commercial illumination tools to identify emerging risks and to ensure that risk management strategies are effectively implemented. They also report about risks, including the likelihood, the consequences, and mitigation progress, to senior management.

2.2. Scope

The focus of the SCRM is shaped by program size, complexity, and budget. The program office should consider focusing on the following:

- readiness drivers
- critical technologies that drive the mission effectiveness of the weapon system, system, product, or service
- components/parts identified in the Program Protection Plan candidate parts list
- mission critical chemicals and materials used to produce, operate and sustain the system
- critical supply chains.

Additional items may be included depending on the program office's expertise, knowledge of the program, and the associated risks to its success. By embracing these responsibilities and focusing on the key areas, the PM ensures that the supply chain remains resilient and capable of effectively managing disruptions to the weapon system, system, product, or service.

3.0 Best Practices

3.1. Plan

All programs should identify supply chain risks and integrate them into the program risk management plan. Ensure that your original equipment manufacturer (OEM) vendors monitor and assess risks early and throughout the system's lifecycle. When supply items are transitioned to the Defense Logistics Agency (DLA) and Service Materiel and Supply Commands, these entities must continue vendor monitoring as part of their materiel management responsibilities. Programs, DLA, and supply and materiel commands should evaluate the cost versus mission risk to determine which items need monitoring. They should also identify readiness drivers, critical technologies, program protection plan candidate parts, mission-critical chemicals and materials, and critical suppliers that will be the focus of continuous SCRM. Consider the following when determining what to monitor:

- materiel complexity
- mission-critical items
- sole source providers
- likelihood of obsolescence
- use of microelectronics from unsecure sources
- parts, materials, and processes management
- prevalence of software, software composition, and software development practices
- restricted vendors
- connections to nation state adversaries
- reliance on rare earth materials
- usage rate
- potential Environmental Protection Agency (EPA), Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) regulations, and Toxic Chemical Substance Act (TCSA) restrictions and
- Army Care of Supplies in Storage (COSIS).

3.2. Illuminate Early

Illuminate risks as early as possible. For a developmental acquisition program, SCRM activities have often been ongoing since the Joint Capabilities Integration and Development System (JCIDS) process or related S&T development. If available, the program office should leverage the SCRM information documented in applicable S&T protection plans as a foundation to build on and should be routinely updated throughout the program's acquisition lifecycle. This early illumination enables informed parts selection and critical decisions before finalizing the system configuration. Once the initial configuration is locked in, implementing changes becomes less flexible, leading to a supply chain that necessitates accepting risks or challenging mitigation actions. However, as the lifecycle progresses, natural opportunities exist for configuration changes, such as modifications and obsolescence mitigations. These changes are opportunities for re-evaluating and reassessing the supply chain. For non-developmental, commercial-off-the-shelf, and services-based acquisition programs, incorporating SCRM criteria during the source selection is essential.

3.3. Share

Share identified high risks in the Program Executive Office (PEO), Systems Commands, Supply and Materiel Commands, Military Service or in an enterprise view to enable everyone to assess impacts across the enterprise more rapidly. A specific high risk could easily be the same material or vendor in many other programs. Illuminate, assess, and share as rapidly as possible to reduce enterprise risk.

3.4. SCRM Process Workflow

Figure 3.0, *SCRM Risk Mitigation Process Flow—Overview* and supporting steps describe the best practice for executing SCRM.

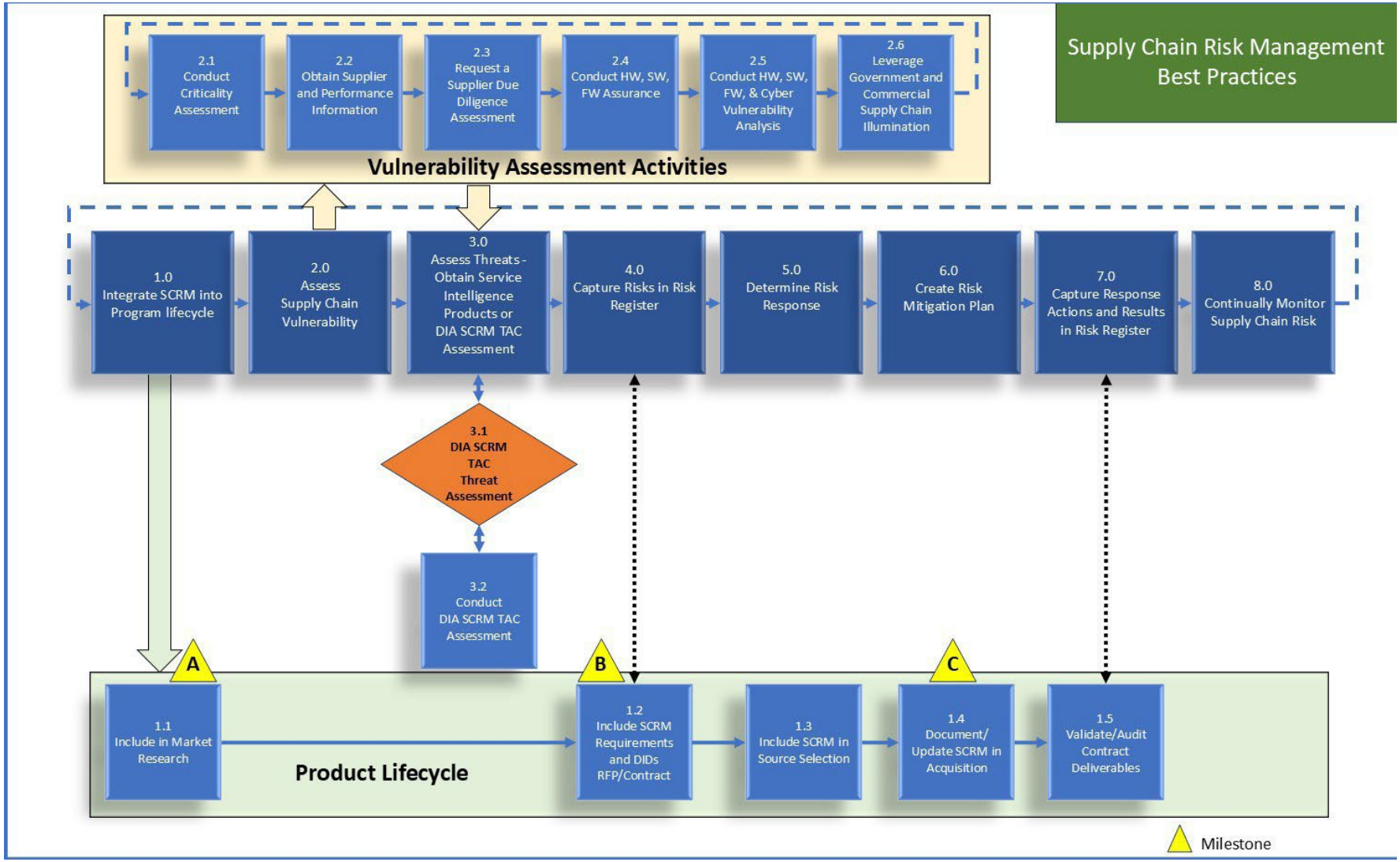

Figure 3.0. SCRM Risk Mitigation Process Flow—Overview

Step 1.0. Integrate SCRM into a Program Lifecycle.

If available, the PM, along with the lead systems engineer and potentially S&T manager, should use the S&T protection plan as a foundation for building the Program Protection Plan (PPP). The S&T protection plan should include critical technology elements and enabling technologies, threats, and vulnerabilities of these items, and selected countermeasures to mitigate associated risks.

Step 1.1. Include in Market Research. Include SCRM in market research to assess potential vendors and, at a minimum, determine if they:

- Provide products and components, or sub-components, sourced through OEM or authorized resellers.
- Have incurred significant malicious network intrusions, data breaches, client data loss, or intellectual property.
- Have an adequate supply chain risk process, plans, controls, and procedures in place to protect the supply chain.
- Have obtained a Cybersecurity Maturity Model Certification (CMMC) level commensurate with the CMMC DFARS guidance at DFARS 204.75 for protection of Controlled Unclassified Information (CUI) for the program.
- Assess Foreign Ownership, Control, or Influence (FOCI) to identify critical geographical vulnerabilities and single-source dependencies.[1]
- Have restricted vendors or connections to nation state adversaries.

Step 1.2. Include SCRM Requirements in Request for Proposal (RFP)/Contract. Develop and include SCRM requirements in the RFP, contracting requirements, including the statement of work (SOW)/statement of objectives (SOO)/performance work statement (PWS), and flow-down requirements. The requirements should ensure the prime contractors, sub-contractors, and suppliers are doing a thorough review for protecting the supply chain and associated war-fighting capabilities. Programs should consider specifying a minimum multi-tiered level SCRM requirements flow-down, particularly for mission-critical systems and subsystems and critical technologies—to properly identify supplier risk early in the program acquisition phase. Many of the entries in Table 5-1, SCRM Mitigation Library, are required. See table 5-1. SCRM Mitigation Library in section 5 of this document.

Step 1.3. Include SCRM in Source Selection. Include supply chain risk as part of solicitation evaluation factors and source selection technical evaluations. Step 2.0. "Assess Supply Chain Vulnerability" should be initiated in parallel to assess vendors before contract award, because lead time is long. SCRM should be explicitly weighed in source selection, with sufficient criteria defined to incentivize the contractor. Consider the following:

- Are evaluators sufficiently skilled, with knowledge of SCRM?
- What training can be provided to enhance evaluators' skills before source selection?
- Can supply chains be monitored continuously by the offeror?
- What SCRM tools are being used by the offeror?

[1] See DoDM 5220.32, Volume 2, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)

- How the offerors provide information to the client (standards, web tool, report, other).
- Company changes that change the risks to operations and maintenance, such as when a prior vendor is added to a restricted vendors list.
- New connections to nation state adversaries.
- Software composition.

Step 1.4. Document and Update SCRM in Acquisition Documents. If available, the PM, along with the lead systems engineer and potentially S&T manager, should use SCRM documentation in the S&T protection plan to inform SCRM responsibilities in the PPP. Document SCRM responsibilities in the PPP and Lifecyle Sustainment Plan (LCSP) unless waived by the Milestone Decision Authority (MDA). At a minimum, document the following in the PPPs:

- How the program will manage supply chain risks to critical program information (CPI), mission critical functions, and critical components.
- When threat assessments will be requested.
- How supply chain threat assessments will be used to influence system design, development environment, and procurement practices and who has responsibility to perform that action.
- If any application-specific integrated circuit (ASIC) requires trusted fabrication.
- How the program will use accredited trusted suppliers of integrated circuit-related services.
- What counterfeit prevention measures will be in place.
- How the program will mitigate the risk of counterfeit insertion during operations and maintenance.
- That the Defense Intelligence Agency (DIA) SCRM Threat Assessment Center (TAC) liaison has been contacted for vendor assessments and provided a critical components list.

Step 1.5. Validate/Audit Contract Deliverables. Regularly analyze content of the Contract Data Requirements List (CDRL) deliverables to ensure they meet the requirements listed for the CDRL and the intent of the deliverable. Update the risk register as needed. Verify that the contractors and subcontractors are fulfilling the requirements (e.g., desk meetings, onsite visits, visiting subcontractors).

Steps 2.0 to 2.6 are different types of SCRM assessments and activities that can be performed if applicable to the program.

Step 2.0. Assess Supply Chain Vulnerability. Assessing supply chain vulnerability will help programs identify the impacts (likelihood of loss) based on the type and level of threat. The activities outlined in steps 2.1 through 2.6 are designed to provide the necessary information for programs to assess supply chain vulnerabilities. Many of these assessments should be done in parallel and the sequence and selection can be tailored to the individual program. When assessing supply chain vulnerability, providing both hardware bills of materials (HBOMs) and software bills of materials (SBOMs) to the entities performing the assessment is crucial. HBOMs detail the components that constitute the hardware, helping to identify subordinate levels of materials and sub-tier suppliers. SBOMs offer comprehensive information about the software code resources that comprise a software package or program. The information includes details about libraries, frameworks, modules, and other elements, enabling better visibility and management of potential vulnerabilities.

Step 2.1. Conduct Criticality Assessment. The program office conducts a criticality assessment to allow the program to focus attention and resources on the system capabilities, mission critical functions and critical components that matter most.

Step 2.2. Obtain Supplier and Performance Information. Remain vigilant of suppliers, or potential suppliers, in the program supply chain by using the Supplier Performance Risk System (SPRS), https://www.sprs.csd.disa.mil/ in accordance with DoDI 5000.79, Defense-Wide Sharing and Use of Supplier and Product Performance Information. SPRS is the authoritative source for retrieving supplier and product performance information assessments for the DoD acquisition community to identify, assess, and monitor unclassified performance. In addition, SPRS provides a list of National Security System restricted suppliers (resulting from section 3252 of Title 10, United States Code determinations), NIST SP 800-171r3, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, "Cyber Security" Assessments (DFARS 252.204-7020), and CMMC certification level (DFARS 252.204-7021). SPRS provides supplier performance scores and procurement risk analysis that include:

- delivery and quality scores based on three years of performance information
- price, item, and supplier risk assessments (includes suspected counterfeit)
- market research, supplier surveillance, and dynamic item risk

Step 2.3. Request a Supplier Due Diligence Assessment. Consider requesting supplier due diligence reports, via commercial and internal sources, which are used for on-demand visibility into supply chain risks when concerned about a supplier, supplier risks are identified, or assistance conducting due diligence on a supplier is needed. Supplier due diligence typically includes the following areas:

- basic company information
- financial information
- cyber hygiene
- third-party risks
- operational risks
- reputational risks

Step 2.4. Conduct Hardware (HW), Software (SW), Firmware (FW) Assurance. Assurance activities ensure the system and components are reliable, secure, and the hardware, software and firmware functions as intended and are free of vulnerabilities, either intentional or unintentional. Conduct HW, SW, and FW assurance activities throughout the life cycle. The Joint Federated Assurance Center will help program offices perform the required activities.

Step 2.5. Conduct HW, SW, FW, and Cybersecurity Vulnerability Analysis. Vulnerability analysis identifies vulnerabilities and assesses vulnerability impact to the system and the system's supply chain. In addition, vulnerability analysis may lead to identifying additional threats, or opportunities for threats, that were not considered in earlier assessments. Much like evolving threats, vulnerabilities change or become evident. Analyze HW, SW, FW, and Cybersecurity vulnerability throughout the life cycle, including development, operational test, operations and sustainment, and disposal.

Step 2.6. Leverage Government and Commercial Supply Chain Illumination. Consider leveraging a government or commercial supply chain capability to illuminate the supply chain and identify risks to software, services, assets, or suppliers and sub-tier suppliers in the supply chain. By using

a commercial supply chain vendor, a multi-tiered supply chain illumination can be done on a specific scope or entire platform using an artificial intelligence-powered software platform to create a supplier repository of all program supplier-buyer relationships from Tier 1–Tier *N* (the commodity/base supplier level).

Step 3.0. Assess Threats - Obtain Service Intelligence Products or DIA SCRM TAC Assessment

Coordinate with the Service/component intelligence community or service/component focal point for Trusted Systems and Networks (TSN) to leverage threat assessments previously identified or to request new threat assessments of companies and entities that require deeper investigation. Threat assessments are typically done by service/component intelligence activities or service/component focal points, and the DIA SCRM TAC is the DoD focal point for these assessments. Reports provided by the intelligence community may be classified as SECRET/NOFORN or higher.

Step 3.1. DIA DoD SCRM TAC Threat Assessment. Program offices should request a DIA SCRM TAC supply chain threat assessment for all Level I and Level II Critical Components (CC)[2] based on their criticality analysis (outlined in step 2.1) for TSN as defined in DoDI 5200.44. Level III & Level IV can often be resolved by TSN service/component focal points and do not require a DoD SCRM TAC assessment.

- Level I criticality is defined as total mission failure.
- Level II criticality is defined as significant/unacceptable mission compromise or system degradation.
- Level III criticality is defined as acceptable partial mission compromise or system degradation.
- Level IV criticality is defined as no mission compromise or degradation.

The DIA SCRM TAC provides due diligence threat assessments of CC and suppliers and informs the program office of the threat level (low, medium, high, critical) and threat confidence (low, medium, high).

Step 3.2. Conduct DIA SCRM TAC Assessment. The threat assessment of a DIA SCRM TAC request is a classified report at least at the SECRET/NOFORN level; some reports may be classified at a higher level due to content.

The classified reports may require some level of evaluation by subject matter experts and intelligence specialists who can help the program office with mitigation options and actions.

Step 4.0. Capture Risks in Risk Register.

The vulnerability assessment (outlined in step 2.0) is coupled with supply chain threat assessments (outlined in step 3.0) to determine the risk. The analysis should include the results of both vulnerability and threat factors in the probability of each occurrence, and the consequence if compromised. Once the risk is defined, mitigation measures should be identified. Assessments of supply chain threat should inform the development of detailed design, test, and evaluation criteria,

[2] Level I components are critical functions and components that have a significant impact if compromised; and Level II components are critical but have a lower impact compared to Level I components.

system-level security risk, and readiness. Programs establish initial risk and use a risk register as a central repository to describe and track risks, as well as to record actions approved by the Risk Management Board (RMB). The risk register also is a tool to quickly sort and filter risks to identify the highest priority ones. A program should develop a risk register as early as possible in its life cycle. The register includes information for each risk, such as risk category,[3] risk statement, likelihood, consequence, planned mitigation measures, the risk owner, work breakdown structure (WBS)/integrated master schedule (IMS) linkage, and, where applicable, expected closure dates and documentation of changes. Programs also may consider combining the risk, issue, and opportunity registers into a single register.

Step 5.0. Determine Risk Response.

Per the DoD *RIO Management Guide*, as risks are identified, the program will develop a strategy to manage risks by evaluating the four risk mitigation options (*accept*, *avoid, transfer, control*) and choose the best option, or a hybrid option.

Step 6.0. Create Risk Mitigation Plan.

Add risk mitigation to the SCRM portion of the program risk mitigation plan. Create a justification for each risk you plan to accept and a mitigation plan (i.e., avoid, transfer, or control) to address each risk deemed unacceptable. The plan or justification should be submitted for stakeholder approval before execution. *Continue to iterate until approved*. Recognize that this is an iterative process so this may take multiple engagements and revisions until stakeholders either conditionally approve or approve the plan. See the *SCRM Strategies* section for further guidance about deciding between the four mitigation options as well as detailed steps for ensuring decisions are properly justified, approved, and documented.

Step 7.0. Capture Response Actions and Results in Risk Register.

Details of any acceptance justification or risk mitigation plan, its execution, and any results going forward should be documented and included in the risk register. The details and results, whether as additional fields aligned with the original risk line item or in a separate database or repository with traceability to the original risk line item, should be included.

Step 8.0. Continually Monitor Supply Chain Risk.

Continually monitor the supply chain for new or imposed risks, threats, and vulnerabilities. Update contract, acquisition documents, and the risk register to reflect changes in supply chain risk activities. Resources for continuous monitoring include:

- Obsolescence/Counterfeit—Government-Industry Data Exchange Program (GIDEP)
- Chemical and Material Risk Management
- DOD Environment, Safety & Occupational Health Network and Information Exchange (DENIX) page for CMRMP that hosts chemical risk alerts (link: https://www.denix.osd.mil/cmrmp/)
- Materials of Evolving Regulatory Interest Team (MERIT) meetings to inform about supply chain impacts created by chemical regulations.
- Environment, Safety and Occupational Health (ESOH)/ESOH IPT

[3] OSD SCRM Taxonomy, March 26, 2025

- NAS 411 Hazmat list to identify chemicals of concern (link: https://standards.globalspec.com/std/14331294/nas411)
- MIL-STD-882E
- DENIX page for ESOH in Acquisition (https://www.denix.osd.mil/esohacq/)
- SCRM Working Group–includes biweekly meetings on SCRM tool demos

4.0 Supply Chain Risk Response Strategies

The *DoD RIO Management Guide* gives guidance about standard options for mitigating risk, including the four mitigation response options: *accept, avoid, transfer*, or *control*. This section contains further guidance about the process of deciding among the four options as well as detailed steps for ensuring decisions are properly justified, approved, and documented.

Figure 3.0 is a guide for creating a mitigation plan/justification after documenting risk in a risk register and determining a response. Below, the section defines each response option and gives an overview of the steps a program or organization should take to properly document their risk mitigation decisions, efforts, and approvals for each option.

Note: The following diagrams are recommended guidance for responding to all risks, but programs and organizations should use discretion for which risks warrant a formal decision-making process. At a minimum, all risks with a high score as assessed by the program/organization, particularly those with a high estimated consequence, should follow this process to ensure all decisions are effectively communicated and agreed on by the relevant stakeholders.

Below are definitions of a few terms present in each option.

4.1. Stakeholders

For each response option, the recommendation is to have an agreed-on list of required stakeholders who will be involved in accepting each mitigation decision, especially for high-risk items. Programs should always follow DoD enterprise risk management guidance (e.g., DoDI 8510.01, *Risk Management Framework for DoD Systems*) when identifying stakeholders for risk-related decisions. In most cases, the list will include the PM, lead systems engineer, and product support manager/lead logistician at minimum. However, stakeholders also can include additional organizations or individuals with significant equity in the results of the decision. For example, if a high risk is identified for a component of a subassembly and the realization of that risk could pose additional significant risk to the subassembly, a representative of the subassembly program should weigh in on the decision to accept, avoid, transfer, or mitigate that risk.

4.2. Approve, Reject, and Conditionally Approve

Document any risk mitigation approval in the system of record, either through case management software or email. If the proposed mitigation option is rejected, the risk owner should return to the decision point and reevaluate which option is best. Conditional approval is not a total rejection but implies the risk owner has not submitted enough substantiation to approve the mitigation option. Therefore, the risk owner should modify the plan or justification, including missing or corrected information, and resubmit. This cycle of conditional approval and resubmission should be repeated until the mitigation option is either approved or rejected.

4.3. Avoid

Avoiding a risk involves taking steps to eliminate the risk entirely or to protect the program from its effects. Avoidance can include changing project plans, processes, or scope to sidestep the risk

altogether. In certain circumstances, excluding a supplier may be appropriate, while also restricting the dissemination of information pertaining to the exclusion.[4]

Figure 4.1 and subsequent descriptions illustrate the steps a program or organization should take to properly document their risk mitigation decisions, efforts, and approvals when choosing to avoid a risk.

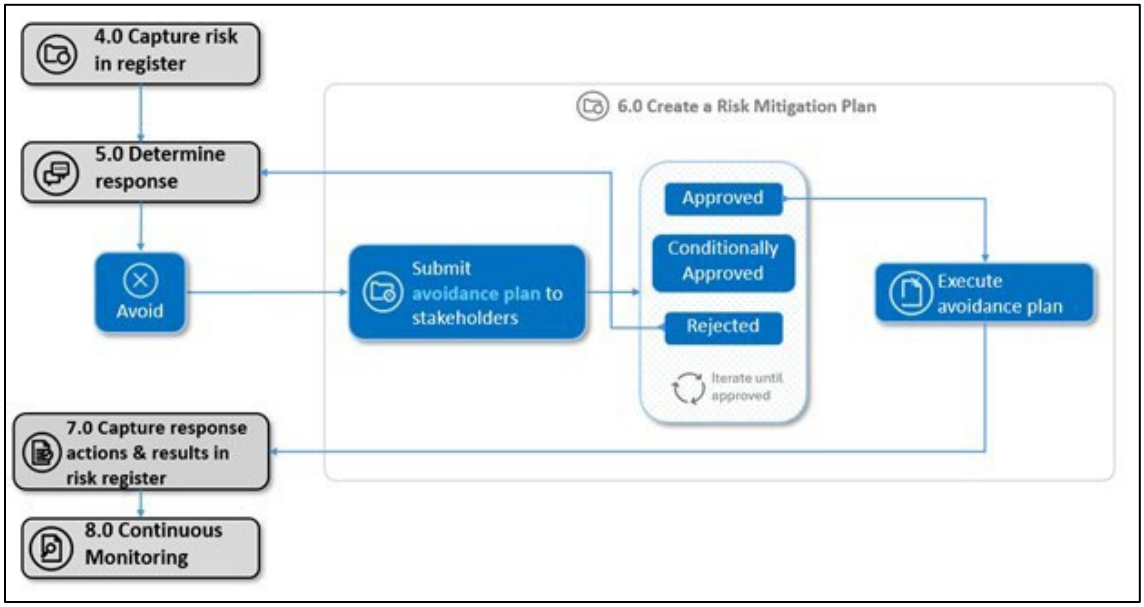

Figure 4.1. Decision Flow for Avoiding a Supply Chain Risk

Figure 4.1. shows how the decision to avoid risk integrates with the overall SCRM risk mitigation process flow detailed in Figure 3.0.

Once the risk owner has decided to avoid the risk, they should document their reasoning in the program risk register and submit their justification to all relevant stakeholders. The justification should include, at a minimum, the following components:

- description of the risk
- risk level, score, and assigned supply chain (SC) risk category[5] (as applicable)
- estimated impact on program cost, schedule, and performance
- estimated likelihood of risk being realized
- courses of action (COAs) for alternate paths to reduce or circumvent the risk
- explanation of how risk will be avoided (i.e., changes to the allocation of program resources, or requirements and specifications) and
- actions that will be taken to monitor risk going forward.

After the required stakeholders have accepted avoidance, the program or organization can follow the planned actions to avoid the risk. Details of the plan, its execution, and results going forward should be documented and included in the risk register—whether as additional fields aligned with the original risk line item or in a separate database or repository with traceability to the original

[4] DoDI 5200.44 implementation of 10 U.S.C. 3252 authorities allow for excluding a supplier while also restricting the dissemination of information pertaining to the exclusion.
[5] DoD SCRM Risk Taxonomy, March 26, 2025

risk line item. The program or organization must continue to monitor the consequences of the avoided risk. If avoidance is unsuccessful and the risk is eventually realized, the results should be reflected and captured in the register as a lesson learned. Similarly, if the avoidance is successful, the results should be captured as well.

4.4. Control

Controlling an SC risk involves implementing measures to reduce the likelihood of the risk occurring or to minimize its impact if it does occur. The measures can involve developing contingency plans, enhancing processes, or applying additional resources to mitigate the risk.

Figure 4.2. and the subsequent description illustrates the steps a program or organization should take to properly document their risk mitigation decisions, efforts, and approvals when choosing to control a risk.

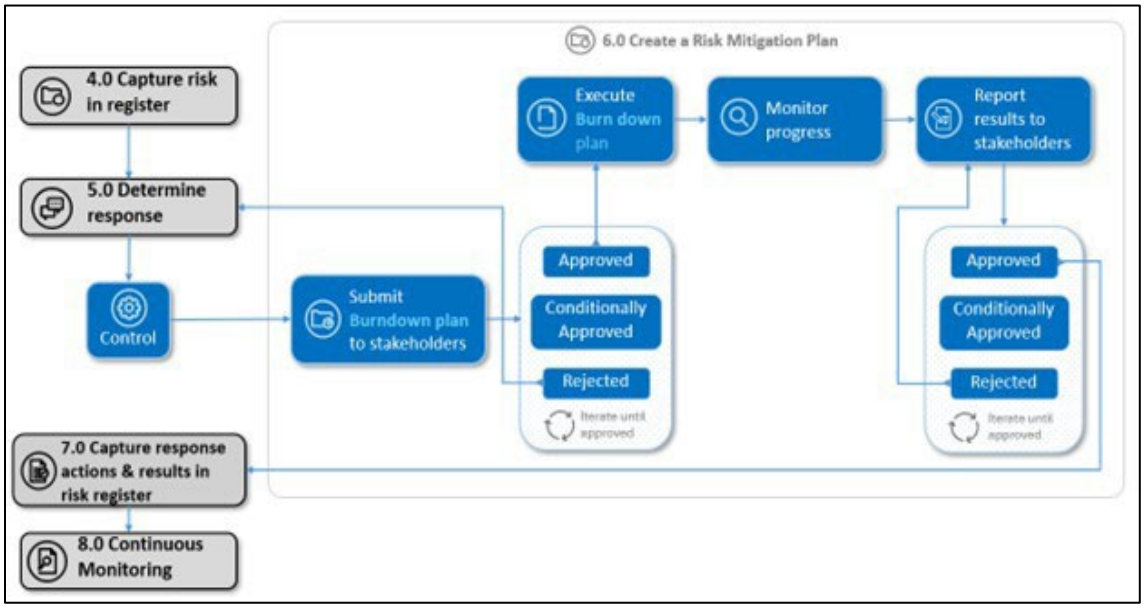

Figure 4.2. Decision Flow for Controlling a Supply Chain Risk

Once the risk owner has decided to control the risk, a risk burndown plan must be created and submitted to all relevant stakeholders for approval. A burndown plan is documentation of planned actions to reduce the risk to an acceptable level (see *DoD RIO Management Guide* for more detail). For low- to moderate-level risks, the plan can include a simple statement summarizing the proposed actions to reduce the risk. For high-level risks, the following components are recommended at minimum:

- description of the risk
- risk level, score, and assigned SC risk category[6] (as applicable)
- estimated impact on program cost, schedule, and performance
- estimated likelihood of risk being realized
- COAs to reduce the risk along with the owner, planned start date, and estimated completion date listed for each action
- each action—clearly defined, objective, and with a specific planned outcome and

[6] DoD SCRM Risk Taxonomy, March 26, 2025

- estimate of how much total risk will be reduced by each action.

Note: The DoD *RIO Management Guide* gives additional guidance for using the burndown plan to track the progress of risk mitigation activities and their quantitative impact on risk. Search for the "risk burn-down" section for more detail.

Once the burn-down plan has been accepted by the required stakeholders, the program or organization will execute the planned actions to reduce the risk and monitor results to ensure the total risk level is reduced per the burndown plan. Once the plan is completed and all actions are complete, the risk owner should submit all results and the final status of the risk to relevant stakeholders for final approval. The results can be in the form of a final report or simple communication (e.g., email) and should include the following components at minimum:

- original risk level and score
- final status of each COA and
- updated risk level and score after burn-down actions

Once the final report has been accepted by the required stakeholders, the program or organization can acknowledge the reduced state of the risk. Details of the burndown plan, its execution, and the final report should be included in the risk register—as additional fields aligned with the original risk line item or in a separate database or repository with traceability to the original risk line item.

The program or organization must continue to monitor for any consequences of the reduced risk. Any significant changes of status or subsequent impact should be captured in the risk register as a lesson learned.

4.5. Transfer

Transferring a risk involves shifting responsibility and sometimes the impact of the risk from one organizational element to another in the supply chain, often by means of contractual requirements. Examples of transferal include outsourcing, procuring insurance, or nominating the risk to be managed by an enterprise-level team (e.g., PEO, headquarters, or the Office of the Secretary of Defense). This shift in responsibility is used when the program or organization lacks the time, capital, or resources required to properly mitigate the risk on their own and another entity is better positioned to manage or absorb it.

Risk can be transferred laterally to another program or organization, vertically to a higher or lower-level entity, or even within a single entity from one individual owner to another. Although complex to manage, risks can also be shared between entities. The transferring and receiving organizational element will often manage risks using different criteria (e.g., sustainment organization may have a larger set of customers and greater demand for the material to ensure readiness across multiple products instead of a program office that is laser focused on the availability and readiness of their product). Nonetheless, both entities should document the transfer and continue to monitor its impact throughout their respective program lifecycles.

Note: to transfer risk, the proposed new owner or organizational element must first agree to receive the transfer. Therefore, ensuring that all appropriate stakeholders from the transferring, receiving, and any higher-level authoritative entities are included as approvers in the transaction is critical.

Figure 4.3. and the subsequent description illustrates the steps a program or organization should take to properly document their risk mitigation decisions, efforts, and approvals when choosing to transfer a risk.

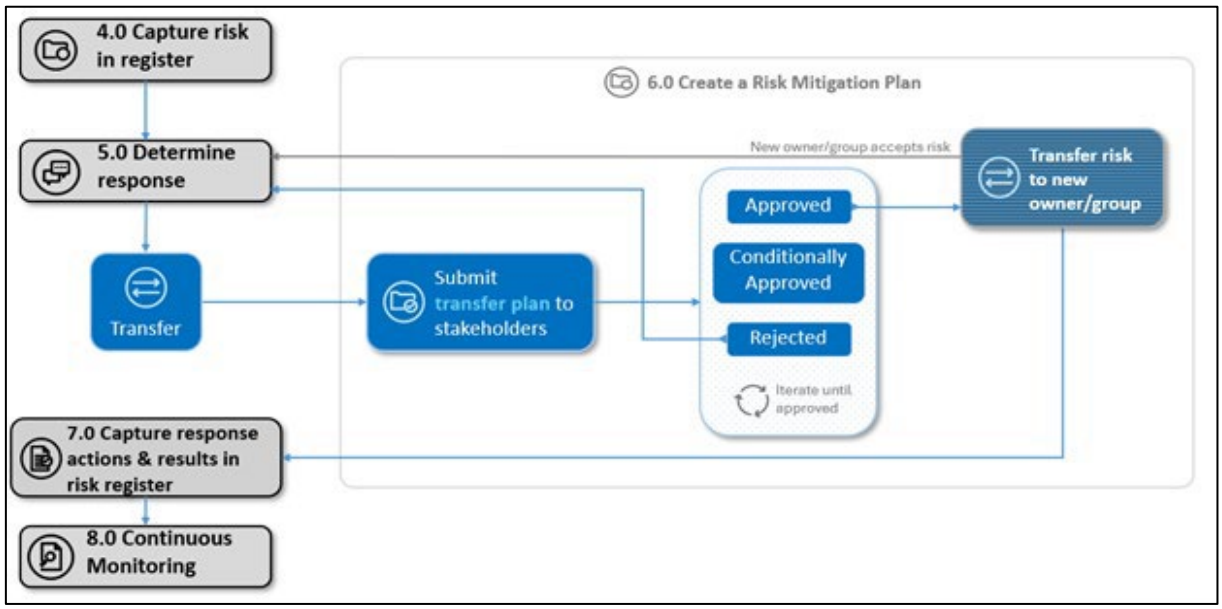

Figure 4.3. Decision Flow for Transferring a Supply Chain Risk

Once general terms have been agreed to by the current risk owner, proposed new owner, the individuals who manage the organizations, a risk transfer plan must be coordinated, documented, and reviewed by all parties. Then, the plan must be submitted to all relevant stakeholders for approval. At a minimum, the plan should include the following components:

- description of the risk
- risk level, score, and assigned SC risk category[7] (as applicable, according to the current risk owner)
- estimated impact on program cost, schedule, and performance
- estimated likelihood of risk being realized
- Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU), detailing the terms of the transfer
- assigned ownership of any potential financial impacts and
- actions each party will take to communicate and monitor for risk status and impact going forward.

Once the required stakeholders accept the transfer plan, the program or organization will follow the planned actions to transfer the risk from the current owner to the future owner. Details of the transfer plan, its execution, and results going forward should be documented and included in the risk register, whether as additional fields aligned with the original risk line item or in a separate database or repository with traceability to the original risk line item. Both programs and organizations must continue to monitor for consequences of the transferred risk. Any significant changes of status or subsequent impact should be captured in the risk register as a lesson learned.

[7] DoD SCRM Risk Taxonomy, March 26, 2025

4.6. Accept

Accepting a risk signifies a collective decision to refrain from taking further action to mitigate the risk, and that the program or organization has decided to accept the consequences of that risk if it is realized. Although this approach is typically reserved for when the risk's potential impact is deemed manageable or when the cost of mitigation exceeds the benefit, it does not imply the risk will be ignored. Accepting a risk implies that it will still be continually monitored to ensure its status or estimated risk level does not change.

Figure 4.4. and the subsequent description illustrates the steps a program or organization should take to properly document their risk mitigation decisions, efforts, and approvals when choosing to accept a risk.

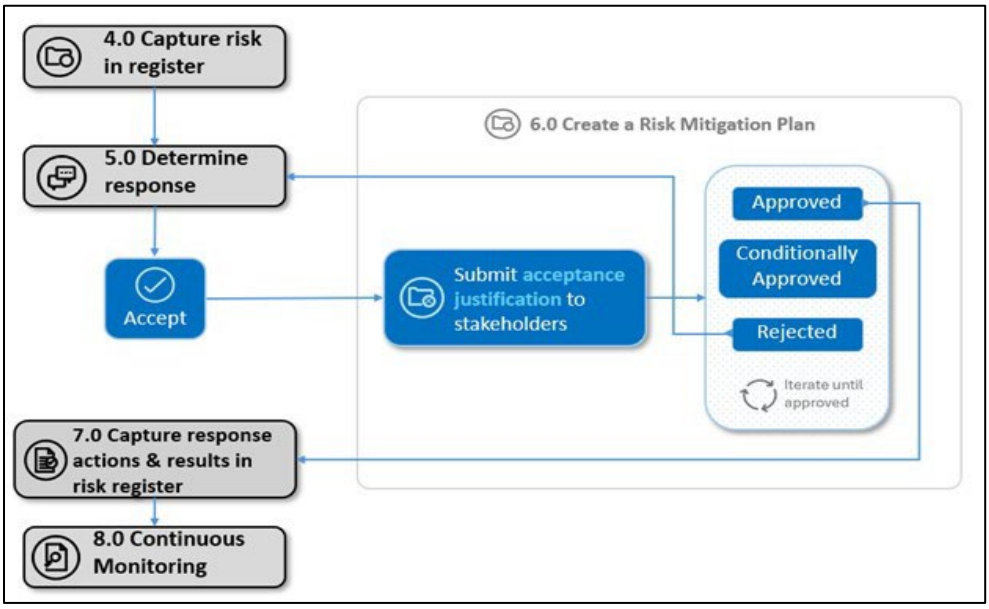

Figure 4.4. Decision Flow for Accepting a Supply Chain Risk

As shown in Figure 4.4., the assigned owner of the risk should document their reasoning for accepting the risk and submit the acceptance justification to all relevant stakeholders. This justification should include the following components at minimum:

- estimated impact on program cost, schedule, and performance.
- estimated likelihood of risk being realized and
- actions that will be taken to monitor risk going forward.

Once the acceptance justification has been accepted by the required stakeholders, details of the risk acceptance and any results going forward should be documented and included in the risk register, whether as additional fields aligned with the original risk line item or in a separate database or repository with traceability to the original risk line item.

The program or organization must continue to monitor for any consequences of the accepted risk. If the risk is eventually realized, the results should be reflected and captured in the register as a lesson learned.

5.0 How to Use the SCRM Mitigation Library, Table 5-1.

Click here to access the library.

Table 5-1, SCRM Mitigation Library can be found at the weblink above. The reader should access the weblink to use while reading the instructions for using the library.

Step 1. Assess your program for what you think are the most critical risk areas based on the type of program you have in accordance with your command or activity risk assessment process. Managing risk of the supply chain should be done as part of your overarching program risk management. Consider starting by identifying subsystem and component *readiness drivers*, *critical technologies* that drive your system's performance, *program protection plan part candidates*, *mission-critical chemicals and materials used to produce the system* and *critical suppliers*. Ensure that SCRM candidates are identified in the program's risk register and document them. As you assess the top candidates in your program risk register, you should categorize the risks using the DoD SCRM taxonomy (*Appendix A*) that includes both major risk categories and sub-risk categories. Identify at least two or more potential major risk categories for each candidate. Once you have categorized the top candidate risks (major risk category level) and documented them in the risk register, you are ready for Step 2.

Step 2. Assess each top SCRM candidate listed in the program risk register and sort the SCRM Mitigation Library (*at link above*) by selecting the top two to three risk areas that you believe are most appropriate to the candidate (based on work in Step 1). We recommend picking a minimum of two risk areas to get a better filtered result. The SCRM Mitigation Library will filter and list potential options and actions you can take to reduce or mitigate the risk.

Step 3. Review the filtered results list and determine which results are the most impactful options and actions. You should start with those options and actions that touch one or more categories, then consider the feasibility of taking an action. First consider the lifecycle phase of the program. Are you early in the program where you can insert contractual requirements to prevent or manage supply chain issues that emerge later? How difficult will it be to add a FAR/DFARS provision or clause or PWS requirement into a contract? What mechanisms will you need to measure effectiveness? If you are in the production or sustainment phase, can you modify the contract and if so, when can this be done? What are the costs and benefits of modifying the contract? How long will it take to achieve the desired results? Should you consider developing a new contract? Do you need Defense Production Act resources to help develop a new source of supply domestically? These are examples of considerations when reviewing the results to determine which options and actions to select. Focus on criticality of candidate and feasibility to make the change. You may select more than one option to pursue.

Step 4. Conduct additional research into the options or actions that you are considering using from the SCRM Mitigation Library. Additional research includes that which helps you understand the supply chain and its intricacies in making holistic informed decisions. Additional research can include finding out how many other programs in your PEO have the same item and risk so you can build a stronger strategy based on increased scale or to elevate the risk to higher headquarters for assistance and resources. Examples of assistance or resources are leveraging solutions that are in place on other programs, identifying how many vendors (domestic and international) can produce

the item, and raw material challenges or competition that limit commercial vendors' production. Use additional research to help you make decisions in Step 5.

Step 5. Determine the appropriate risk response using your risk management plan and the analysis of the SCRM Mitigation Library results and additional research. Each of the four risk management strategies are the outputs of the SCRM process. Some may include actions outlined in the SCRM Mitigation Library, such as adding a reference, Data Item Description, or FAR/DFARS provision or clause in your contract to help lay the foundation in the contract to mitigate supply chain risks in the future.

Appendix A. DoD Supply Chain Risk Management Taxonomy

The following are the DoD Supply Chain Risk Management key term definitions and risk mitigation categories; the full Taxonomy is at: https://www.acq.osd.mil/asds/log/index.html

Term	Definitions
Supply Chain (SC)	The linked activities associated with providing material to end users for consumption. Those activities include supply activities (such as organic and commercial inventory control points (ICPs) and retail supply activities), maintenance activities (such as organic and commercial depot level maintenance facilities and intermediate repair activities), and distribution activities (such as distribution depots and other storage locations, container consolidation points, ports of embarkation and debarkation, and ground, air, and ocean transporters).
Supply Chain Management (SCM)	Meeting customer-driven materiel requirements through the acquisition, maintenance, transportation, storage, and delivery of materiel to customers, and managing materiel returns, movement of reparable materiel to and from maintenance facilities, and ensuring the exchange of information among customers, maintainers, supply chain managers, and suppliers.
Supply Chain Risk Management (SCRM)	The systematic process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions throughout the supply chain and implementing mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as threats are identified or disruptions occur.

Risk Mitigation Category	
1	Regulatory and Compliance
2	Manufacturing & Supply
3	Foreign Ownership, Control, or Influence (FOCI)
4	Political
5	Technology & Cybersecurity
6	Financial
7	Economic
8	Product Quality & Design
9	Human Capital
10	Transportation & Distribution
11	Environmental
12	Infrastructure

Appendix B. DoD Supply Chain Risk Management Policy Intersection

B-1. Policy Intersection. Figure B-1 highlights the intersection of key SCRM policies and guidance in three major areas: (1) Acquisition and Science and Technology, (2) Materiel Management and (3) Defense Industrial Base. Program offices should consider that SCRM is driven by several perspectives and policy proponents. See tables B-1 through B-3 for detailed listings.

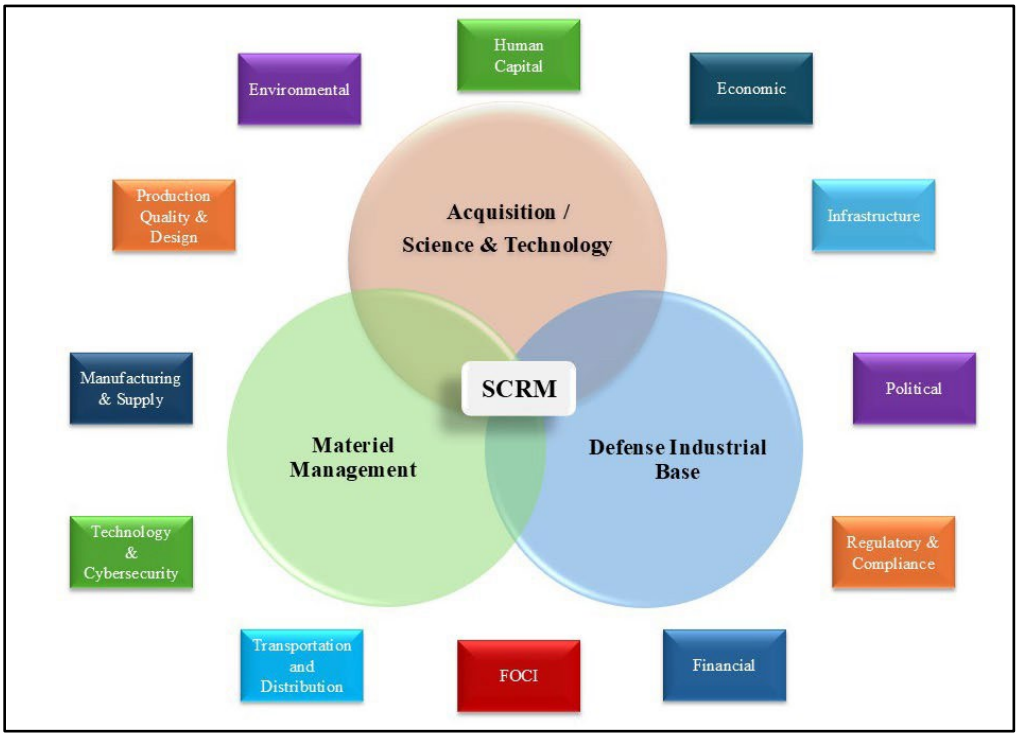

Figure B-1. SCRM Policy Intersection

Materiel Management Policies Related to SCRM	
DoDD 5105.22	Defense Logistics Agency
DoDI 4140.01	DoD Supply Chain Materiel Management Policy, Volumes 1, 2, 3, 4, 5, 6
DoDM 4140.01	DoD Supply Chain Materiel Management Procedures, Volumes 1, 2, 3, 4, 5, 6
DoDI 4140.67	DoD Counterfeit Prevention Policy
DoDI 4715.18	Emerging Chemicals of Environmental Concern
DoDI 5200.49	Oversight of the Collection and Exchange of Information Using the Government-Industry Data Exchange Program (GIDEP)
SD-25	GIDEP Operating Policies and Procedures
DoDI 4245.15	Diminishing Manufacturing Sources and Materiel Shortages Management (DMSMS)
DoDM 4245.15	Management of Diminishing Manufacturing Sources and Material Shortages
SD 19	Parts Management Guide (Oversight of parts Selection)
SD 22	DMSMS Guidebook
SD 26	DMSMS and Parts Management Contracting Guide

Acquisition, Science & Technology Policies Related to SCRM	
EO 14028	Improving the Nation's Cybersecurity
DoDI 5000.02	Operation of the Adaptive Acquisition Framework
DoDI 5000.75	Business Systems Requirements and Acquisition
DoDI 5000.80	Operation of the Middle Tier of Acquisition
DoDI 5000.85	Major Capability Acquisition

Acquisition, Science & Technology Policies Related to SCRM	
DoDI 5000.87	Operation of the Software Acquisition Pathway
DoDI 5000.91	Product Support Management for the Adaptive Acquisition Framework
DoDI 5000.79	Defense Wide Sharing and Use of Supplier and Product Performance Information (PI)
DoDI 5000.82	Requirements for the Acquisition of Digital Capabilities
DoDI 5000.83	Technology and Program Protection to Maintain Technological Advantage
DoDI 5200.39	Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
DoDI 5200.44	Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
DoDD 5200.47E	Anti-Tamper (AT)
DoDI 8500.01	Cybersecurity

Defense Industrial Base Policies Related to SCRM	
50 USC, Chap 55	The Defense Production Act
EO 14017	America's Supply Chain
DoDM 5200.32, Vol I	National Industrial Security Program, Industrial Security Procedures for Government Activities, located within 32 CFR Part 117
DoDI 2000.25	DoD Procedures for Reviewing and Monitoring Transactions for the Committee on Foreign Investment of the United States
DoD 4400.1-M	Department of Defense Priorities and Allocation Manual
DoDI 5000.60	Defense Industrial Base Assessments
DoDD 5101.18E	DoD Executive Agent for Printed Circuit Board and Interconnect Technology

Acronyms

ASIC	Application-Specific Integrated Circuits
CC	Critical Components
CDRL	Contract Data Requirements List
COA	Course of Action
CPI	Critical Program Information
CMMC	Cybersecurity Maturity Model Certification
C-SCRM	Cyber-Supply Chain Risk Management
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoDI	Department of Defense Instruction
DMSMS	Diminishing Manufacturing Sources and Material Shortages
EO	Executive Order
ESOH	Environment, safety and occupational health
FAR	Federal Acquisition Regulations
FW	Firmware
HW	Hardware
IT	Information Technology
IMS	Integrated Master Schedule
LCSP	Lifecyle Sustainment Plan
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MDA	Milestone Decision Authority
NIST	National Institute of Standards and Technology
NSS	National Security System
OEM	Original Equipment Manufacturer
PWS	Performance Work Statement
PEO	Program Executive Office
PM	Program Manager
PPP	Program Protection Plan
RIO	Risk, Issue, and Opportunity
RMB	Risk Management Board
SC	Supply Chain
SW	Software
SP	Special Publication
SOO	Statement of Objectives
SOW	Statement of Work
SPRS	Supplier Performance Risk System
SCRM	Supply Chain Risk Management
TAC	Threat assessment Center
TSN	trusted systems and networks
WBS	Work Breakdown Structure