NPS-LM-23-031

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Risky Business: An Analytical Approach to Services Supply Chain Risk Management

December 2022

Capt Christopher J. Graham, USAF
Capt Leila Rahebi, USAF

Thesis Advisors: LtCol Daniel Finkenstadt, Assistant Professor
Michael Ripley, MITRE

Department of Defense Management

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Department of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact the Acquisition Research Program (ARP) via email, arp@nps.edu or at 831-656-3793.

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

ABSTRACT

Cyber threats, economic upheavals, and environmental disasters threaten global supply chains. These vulnerabilities impact the readiness of U.S. forces and their capacity to defend the nation. Consumers and the government need a framework for assessing vulnerabilities and establishing effective supply chains. MITRE's System of Trust (SoT) serves as a framework to measure trustworthiness and identify risk factors affecting their supply chain security. The SoT develops a taxonomy of risk factors, defines risk measures attributable to those risk factors, and creates a framework for organizations to objectively quantify supply chain risk. Our study validates the services risk factors and identifies techniques and best practices to mitigate risk unique for services. Our research questions are: What are the primary indicators of supply chain risk, and which are unique to Department of Defense services? Furthermore, what are the best practices for preventing, mitigating, and responding to service-specific supply chain risks? This research draws on qualitative interview data to obtain insight into the services aspect of supply chains, systematically evaluate MITRE's risk factors and risk measures, and identify gaps in available data. Our research results in a Services Supply Chain Risk Management Framework that managers should use to evaluate and mitigate risks within their supply chains.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank all those who volunteered to participate in our study. Their experiences and insight into real challenges they face dealing with supply chains were invaluable and instrumental to our research. Next, we would like to thank the MITRE Corporation for partnering with us to develop a research topic. The many discussions we participated in allowed us to tangibly contribute to the development of the System of Trust Framework and receive feedback throughout the course of our research. Particularly, we need to thank Michael Ripley (Rip), our second reader, for his patience, guidance, and transparent communication. Rip was instrumental in teaching us about the System of Trust and made sure we were included in all of MITRE's discussions about the framework. We also want to thank Lieutenant Colonel Daniel Finkenstadt, our advisor, for his notable support, leadership, and mentorship. Lt Col Finkenstadt played so many roles in our time at NPS. He served as our instructor, advisor, and mentor. We could not have produced this report without his pedagogy and expertise. Finally, we want to thank our families for their love and support throughout our educational journey.

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-LM-23-031

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Risky Business: An Analytical Approach to Services Supply Chain Risk Management

December 2022

Capt Christopher J. Graham, USAF
Capt Leila Rahebi, USAF

Thesis Advisors: LtCol Daniel Finkenstadt, Assistant Professor
Michael Ripley, MITRE

Department of Defense Management

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACC	Air Combat Command
AFCENT	Air Forces Central
AFICC	Air Force Installation Contracting Center
AFLCMC	Air Force Life Cycle Management Center
AFPEO/CM	Air Force Program Executive Office for Combat Mission Support
AMIC	Acquisition Management and Integration Center
CAF/CAS	Combat Air Forces/Contracted Air Support
CI	Counterintelligence
COR	Contracting Officer Representative
CPARS	Contractor Performance Assessment Reports
CRADA	Cooperative research and development agreement
CSIS	Center for Strategic and International Studies
DIB	Defense Industrial Base
DLA	Defense Logistics Agency
DOD	Department of Defense
DoL	Department of Labor
EITaaS	Enterprise Information Technology as a Service
FAR	Federal Acquisition Regulation
FFRDC	Federally funded research and development centers
FIE	Foreign intelligence entities
GAO	Government Accountability Office
HAF	Headquarters Air Force
ICOPARS	Internet-Based Contractor Operated Parts Store
IDIQ	Indefinite Delivery Indefinite Quantity
KBS	Knowledge-based services
KTR	Contractor
MCIO	Military Criminal Investigative Organizations
NAVAIR	Naval Air Systems Command
PSC	Product Service Code
PWS	Performance Work Statement

QASP	Quality Assurance Surveillance Plan
RMM	Risk Model Manager
SaaS	Software as a Service
SCOR	Supply Chain Operations Reference
SCR	Supply Chain Resilience
SCRM	Supply Chain Risk Management
SME	Subject Matter Expert
SoT	System of Trust
SOW	Statement of Work

I. INTRODUCTION/ MOTIVATION

Supply chains are a critical vulnerability to the Department of Defense (DOD) warfighting capability. Supply chains have been susceptible to global disruptions, cyber threats, material shortages, delays, economic upheavals, environmental disasters (Schiffling & Kanellos, 2022). These vulnerabilities continue to impact the readiness of our forces and the capacity to defend the nation. The DOD needs to proactively identify risks within its supply chain to sustain global readiness and efficiently deliver critical requirements to the warfighter. Two recent examples, the Colonial Pipeline ransomware attack (Reeder & Hall, 2021) and the SolarWinds attack (Whitaker, 2021) highlight the threat adversaries pose to U.S. supply chains. The Center for Strategic and International Studies (CSIS) publishes a timeline of significant cyber-attacks. In June 2022 alone, they recorded 12 attacks targeting government agencies and defense or technology companies, with each attack resulting in a loss exceeding one million dollars (Center for Strategic and International Studies [CSIS], 2022).

Supply chains are foundational for value-added manufacturing and the effective delivery of essential services. Supply chain managers strive to create agile, adaptable, and aligned supply chains. Agile supply chains quickly adjust for disruptions. Adaptable supply chains enable flexibility to modify processes and reinforce adjustments to longer shifts in the market. Alignment connects the entire supply chain to maximize performance. Within Military Criminal Investigative Organizations (MCIO), procurement fraud and counterintelligence disciplines are becoming more intertwined. Foreign intelligence entities (FIE) increasingly target DOD acquisition and supply chains to subvert DOD innovation efforts and readiness. In 2021, the Government Accountability Office (GAO) published recommendations urging agencies to take action to manage supply chain risks (Harris, 2020). The GAO warned without supply chain risk management (SCRM) processes, agencies are vulnerable to malicious actors. In addition, the COVID-19 pandemic revealed critical vulnerabilities and gaps in U.S. supply chains. Industry and the DOD still struggle to create a resilient supply chain. In 2021, President Biden requested a

review of U.S. supply chains as a response to the vulnerabilities resulting from the COVID-19 pandemic (White House, 2021).

The MITRE Corporation, a company operating six federally funded research and development centers (FFRDC), started development of a framework, known as the System of Trust (SoT), to establish a measure of trustworthiness between organizations based on identified risk factors that could disrupt an organization's supply chain (Martin et al., 2021). The goal of the SoT is to develop a taxonomy of supply chain security risk factors, define risk measures attributable to those risk factors, and create a tailorable tool for organizations to use to objectively quantify supply chain risk. This will allow organizations to curtail consequences and potential disruptions that could result from failure to identify and address risks.

MITRE separates the supply chain into three aspects, suppliers, supplies, and services. The SoT defines suppliers as "an organization or entity that provides supplies and /or services" (M. Ripley, personal communication, November 1, 2022). The definition for supplies is "a particular physical or digital object, entity, part, component or material" (M. Ripley, personal communication, November 1, 2022). Finally, the SoT defines services as "a particular activity that is required for a supply chain to function" (M. Ripley, personal communication, November 1, 2022). Within a supply chain, all three aspects play a role in delivering the final good or service and each aspect carries risk. The SoT contains a robust security risk taxonomy on supplies and suppliers, with extended and well-established research. Yet, from an academic standpoint, the focus in supply chain management has been predominantly on goods-related logic and empirical research on services-focused supply chain is scarce. We chose to focus our research specifically on the services aspect of supply chains for two principal reasons. First, in fiscal year 2020, services contracting accounted for 51% of the $420 billion budget for DOD contracts (Peters, 2021). Second, evaluating services presents a unique challenge to business managers because services are heterogeneous and cannot be replicated by a manufacturing process with inputs and outputs. The unique characteristics of a service include the intangibility of service outcomes and the participation of customers (Apte et al., 2006). Because of the complexity

in evaluating services and the large portion of the DOD's budget dedicated to services, managers need a validated tool to analyze risks within the services supply chain.

A. STATEMENT OF THE PROBLEM

The complexity of managing services supply chains creates challenges for managers and relies on their ability to understand the risk factors and subfactors as well as risk prevention and mitigation techniques to respond to challenges and create agile, aligned, and adaptable supply chains.

B. PURPOSE OF THE STUDY

Through a cooperative research and development agreement (CRADA) collaboration with MITRE, our research results will inform the SoT Framework. Our research questions are:

- RQ1: What are the primary indicators of supply chain risk, and which are unique to DOD services?
- RQ2: What are the best practices for preventing, mitigating, and responding to DOD service specific supply chain risks?

C. OVERVIEW OF THE STUDY

The literature review consisted of collecting, analyzing, and interpretting data from news articles, defense reports, scholarly publications, and online journals relating to services, supply chain risk management, and resilience mitigations. Upon further analysis of the literature, we conducted interview with Subject Matter Experts (SME) and related-industry professionals. We then used a thematic analysis approach to examine the qualitative data to provide insights to recommendations and process areas (Creswell & Poth, 2018).

D. CONCLUSION

The DOD consistently seeks ways to improve and modernize its supply chain resilience. In response to a global pandemic that exposed massive global supply chain

vulnerabilities and the subsequent Presidential Executive Order 14017, Executive Order on America's Supply Chains (Executive Order No. 14017, 2021), an action plan titled *Securing America's Supply Chains* was published calling for a healthy, resilient, diverse, and secure supply chain for the DOD. (DOD, 2022). While the action plan focused strictly on supply chains in the Defense Industrial Base (DIB), it highlighted further need to examine internal organizations within the DOD that held a key role in supply chain resiliency. The services aspect of supply chains presents a critical challenge to acquisition professionals in an uncertain and everchanging world. Services add to the complexity in supply chain risk management. Not only are the supply chain networks complex, as with products, but the resources, delivery methods and standards are highly variable and subject to idiosyncrasies that further complicate the government's ability to monitor and manage them effectively. Our research addresses this problem by identifying a taxonomy of risk factors and subfactors specific to the services aspect of supply chains.

II. BACKGROUND/LITERATURE REVIEW

A. BACKGROUND

The necessity of methodologies and frameworks for managing supply chain activities and processes is not new. The motivation for the SoT came from a ubiquitous need to address supply chain security (Martin, 2020a). The COVID-19 pandemic unveiled vulnerabilities in companies with fragile supply chains, while other companies who were able to adapt, increased revenues (Veselovska, 2020). Organizations rely on trustworthy suppliers to respond to supply chain disruptions. The SoT responds to these concerns by addressing the barriers to trust between organizations (Martin, 2020a). Boer et al. identifies the need for different approaches for managing the supplier selection process, allowing strategic value for organizations (2001).

1. Defining Supply Chain Risks

Several definitions of supply chain risks exist and may vary depending on the context or industry. To be able to examine supply chain risks, we need to establish a working definition of a supply chain for our research. Cooper and Ellram define a supply chain as the flow, from supplier to user, along a distribution channel (1993). La Londe and Masters offer a more supplier oriented definition referring to a supply chain as the set of firms which pass the materials forward (1994). Furthermore, the DOD Supply Chain Material Management Policy defines a supply chain as the activities associated with providing materiel to end users for consumption (Department of Defense [DOD], 2019). Our paper uses a derivative of these definitions when referring to supply chains. For this paper, a supply chain will refer to the activities involved in the flow of goods, and services from sourcing raw materials to delivering to a customer and final disposal. Using a broad definition allows for the consideration of risks along any point of the supply chain.

Private industry and the DOD have differing views on risk, stemming from different objectives. In industry, with the objective to make a profit and increase cash flows, supply chain risks may be seen as any disruptions that affect profitability (Chopra & Meindl, 2013). Others see supply chain risk as a risk affecting the flow of supplies to the end user

(Juttner et al., 2003). This definition focuses on the demand matching the supply of goods and services. The Risk Management Guide for DOD Acquisition defines risk as "a measure of the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints" (Defense Acquisition University, 2003, p. 7). This guide views risk as having two components: the probability of the risk occurring, and the impact of realizing that risk on cost, schedule, or performance (Defense Acquisition University, 2003). Our research explores the supply chain risk factors within the DOD and as such, will adapt this DOD definition of risk.

2. System of Trust

The SoT seeks to provide a framework to standardize how organizations assess supply chain risk and address barriers of trust among suppliers, supplies, and services (Martin, 2020b). To accomplish its SoT goal, MITRE identified four lines of effort (Martin et al., 2021):

- Create a taxonomy of the barriers to trust between organizations regarding supplies, suppliers, and services
- Identify ways to gather evidence relating to those concerns
- Allow the SoT to be tailored to specific concerns faced by organizations
- Create an objective method to score risk and assign a value to the risk (Martin et al., 2021)

This will allow organizations to curtail consequences and potential disruptions that could result from failure to identify and address supply chain security risks. Organizations will be able to tailor the SoT to fit their own needs and industry so it can be applied to government agencies as well as private sector industries.

3. SoT Risk Areas

The SoT identifies three aspects of trust to a supply chain for risk analysis, suppliers, supplies, and services. Within these aspects, the SoT identifies risk areas for

evaluation to establish trust between organizations. Within the services component, the risk areas include security, reliability, quality, and integrity (Ripley, 2021). Table 1 lists the SoT definitions for these risk areas.

Table 1. Risk Area Definitions. Source: M. Ripley (personal communication, August 1, 2022).

Security	The extent to which something maintains its intended properties in the face of intentional malicious action
Reliability	The extent to which something maintains an expected level of quality over a defined time interval
Quality	The extent to which something conforms structurally and functionally, within the expected environmental or usage parameters; fitness for intended use
Integrity	The extent to which something remains complete, unmodified, unimpaired, and uncorrupted from its intended form

To further illustrate these definitions, consider a local government hires a contractor to add a lane to a highway to ease the flow of traffic. Involved in the project are suppliers, to include all the second and third tier suppliers, the supplies needed to build the road, and finally the services involved in the construction. These services may include the transportation of the supplies and the physical construction services. The security risk areas gauges how susceptible the construction service is to external or malicious influences. The reliability risk area gauges if the customer can trust the construction service to build a road and on time. The quality risk area gauges how the construction met the customer's perceived quality standards. Finally, the integrity risk area gauges how well the service aligned to the overall objective, in this case easing the flow of traffic (M. Ripley, personal communication, July 25, 2022).

Within the risk areas, MITRE identifies risk factors which signal problems. To assess the risk factors, MITRE developed risk measures which are yes/no questions (Martin et al., 2021). These yes/no questions are the user inputs into the tool which the tool then analyzes and outputs a quantitative score for the risk factors. Using binary inputs minimizes the amount of analysis the user needs to perform when using the tool (Martin et al., 2021).

Figure 1 illustrates the relationships between risk measurements with risk factors and risk categories. The entire structure of the SoT can be found in Appendix A.

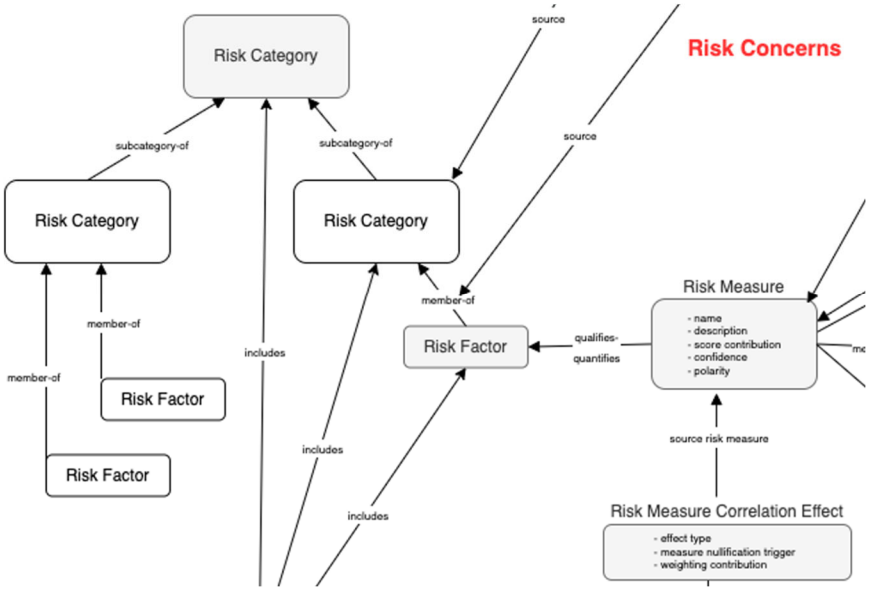


Figure 1. SoT Basic Structure.
Source: M. Ripley (personal communication, September 12, 2022).

Consider again the example of the local government hiring a contractor to add a highway lane. The reliability risk area includes risk categories, one of which may be the construction specific reliability. The availability of qualified technicians could be a risk factor underneath this category. This risk factor could be measured by the number of certified technicians or the attrition rate at the company. Appendix B shows the current work-in-progress top-level categories of risk.

To leverage SoT, MITRE is building a tool called the Risk Model Manager (RMM). Within this tool, a user first selects the type of analysis they are conducting and what data they have access to (Ripley, 2021). This focuses the context of the analysis appropriate to the user's needs. A user may use this tool to assess their own supply chain. Users assessing their own supply chain will be able to feed the tool more accurate inputs, thus providing a better sight picture as compared to assessing external organizations with limited data. A user may also evaluate an external organization relying on open-source data (Ripley, 2021).

The tailor-ability of the SoT allows the user to select the data they have access to, whether they are reliant on open-source data or have conducted discussions with their supplier. There is an inherent limitation of relying on open-source data, the analysis may be incomplete, inaccurate, or obsolete. As with any tool, the performance of the SoT relies on the user inputs. The data quality limits the level of analysis the tool can perform.

4. Conclusion

This section introduces the SoT and provides an overview of the current taxonomy structure. The SoT is the taxonomy of risk areas and risk factors, while the RMM is the tangible tool for users to assess their supply chain based off the SoT framework. Additionally, more background is given regarding the services aspect of the System of Trust and the way MTIRE currently defines its categories and subcategories. The next section will review the research previously conducted regarding supply chain risks, services, and supply chain risk management techniques.

B. LITERATURE REVIEW

1. Different Types of Supply Chain Risk

Reasons for supply chain disruptions have been extensively studied and literature has classified a wide-ranging variety of supply chain risks. Shashi et al. (2020) asserts that there are two types of supply chain risks. The first, operational risks, considers economic uncertainties such as supply and demand. The second, disruption risk, refers to disruptions caused by natural disasters or labor strikes. According to Shashi et al., operational risks are more common but have less severe impacts, whereas disruption risks are not as frequent but have greater economic and societal consequences (2020). However, since the COVID-19 pandemic, disruption risks have become more ubiquitous (Schiffling & Kanellos, 2022). Both operational and disruption risks could gravely interrupt and delay materials, information, cash flows, which could further erode profits, increase costs, and cause a whirlwind of negative effects for an organization (Shashi et al., 2020).

Recently, business organizations and communities have found themselves in more risky and uncertain situations. Internal instability, economic and political factors, and

environmental disasters are all sources of risk for today's business community (Guinto, 2022). Further, foreign intelligence entities and counterfeiters threaten the integrity of organizations' data and systems (Harris, 2020). Aqlan and Lam (2015, p. 54) identify three main factors contributing to supply chain vulnerability and risk: "(1) globalization of sourcing, production, and sales, (2) increased complexity and competitiveness, and (3) occurrence of internal and external risk events such as material shortages and natural disasters." Chopra and Sodhi (2004, p. 54) categorized potential supply chain risks into nine categories (as demonstrated in Table 2): "(1) Disruptions, (2) Delays, (3) Systems, (4) Forecast (5) Intellectual property (6) Procurement (7) Receivables (8) Inventory and (9) Capacity."

Table 2. Categories of Risk. Adapted from Chopra and Sodhi (2004).

Category of Risk	Risk Drivers
Disruptions	• Natural disaster • Labor strikes • Supplier bankruptcy • War & terrorism • Dependence on a single source of supply and the capacity & responsiveness of alternate suppliers
Delays	• High-capacity utilization at supply source • Inflexibility of supply source • Poor quality at supply source • Excessive handling due to border crossings or changes in transportation modes
Systems	• Information infostructure breakdown • System integration or extensive system networking • E-commerce
Forecast	• Inaccurate forecasts due to long lead times, seasonality, product variety, short life cycles, small customer base • Information distortion due to sales promotions, incentives, lack of supply chain visibility & exaggeration of demand in times of product shortage
Intellectual Property	• Vertical integration of supply chain • Global outsourcing & markets
Procurement	• Exchange rate risk • Percentage of a key component or raw material procured from a single source

Category of Risk	Risk Drivers
	• Industrywide capacity utilization • Long term vs short term contract
Receivables	• Number of customers • Financial strength of customers
Inventory	• Rate of product obsolescence • Inventory holding cost • Product value • Demand & supply uncertainty
Capacity	• Cost of capacity • Capacity flexibility

Individual risks are frequently interrelated, making supply-chain risk management complex. As a consequence, efforts intended to alleviate one risk may instead exacerbate another. Based on the research from Chopra and Sodhi (2004), supply-chain risks can quickly escalate into full-fledged supply-chain problems, resulting in unplanned changes in flow as an impact of interruptions or delays. In their most recent book, *Flow: How the Best Supply Chains Thrive*, Handfield and Linton identify that supply chains as fast, agile, fluid systems that sense, respond, and navigate autonomously (2022). To thrive and obtain optimum efficacy, supply chains need to be released from control and flow as freely as possible (Handfield & Linton, 2022). If supply chains do not flow, colossal problems emerge, including shortages, economic shutdowns, and medical emergencies (Handfield & Linton, 2022).

Supply chain disruptions, while they could be benign, may significantly disrupt an organization's processes (Chopra & Sodhi, 2004). For example, a simple instrument malfunction on an assembly line may create a significant bottleneck and impact not only the factory's manufacturing, but also the supply chain of any higher tier manufacturer. The authors argue most businesses create policies to safeguard their supply networks against recurring, low-impact risks. Whereas, other firms almost completely disregard high-impact, low-probability risks. The above example shows how companies need to actively manage their supply chains and assess risk at all levels of the supply chain.

2. Services

In 2021, services comprised 87% of employment in the U.S. (Department of Labor [DoL], 2022a). Despite representing the majority employment, most available research regarding supply chain risks relate to supplies and suppliers. Services differ from supplies and, as a result, it is difficult for customers to evaluate service quality. The federal government, arguably the largest customer for services, attempts to handle these risks through its governing regulations regarding contracting. The available literature discusses the challenges regarding services supply chains and the current risks factors.

a. Nature of Services

The U.S. Bureau of Labor Statistics divides service jobs into the following categories: "trade and utilities, information services, financial activities, professional and business services, education and health services, leisure and hospitality, other services, and government" (DoL, 2022b, p. 1). Services distinguish themselves from supplies in several ways. Apte et al. researched the challenges services present to the DOD and explained how services differ than managing supplies (2006). Services, they found, distinguish themselves by their unique characteristics which include the intangibility of output, heterogeneous nature, the difficulty of portability, and complexity in measurement. Also, they noted, services may include input from both the buyer and the seller. Law enforcement, for example, includes input from both the officer as well as private citizens, the "buyer." Additionally, services are inseparable from their source of production meaning they are created at the point of use (Ellram et al., 2007).

Despite these characteristics, similar considerations when managing supplies are taken when managing services. This is because services may rely on an inventory of supplies. The police officer requires supplies such as a vehicle and uniform to successfully perform the law enforcement function. However, Apte et al. acknowledged the intangible inputs, which distinguish services, are difficult to measure because they may come from both the buyer and the seller (2006). Christian Gronroos expands on Apte et al.'s definition including services as activities, or a series of activities, and notes services are consumed and produced simultaneously (1988). Haywood-Farmer also presents his identified special natures of

services in his work regarding service quality (1988). In addition to what others have stated, he identified production workers as marketing tools in the service sector (Haywood-Farmer, 1988). He argues because of the customer interaction, services use their employees to signal quality to potential customers. Goods manufactured in large factories lack this aspect. All the research regarding services converges on similar themes. In summary, services differ from supplies because they are complex, heterogeneous, and intangible, involving input from both the buyer and seller (co-production/co-creation). Also, services are perishable, as they are consumed as they are produced.

b. Service Quality

After defining what a service is, it is important to understand how services are measured. Services involve interactions with customers and are intangible, so their measurement will be subjective. Service quality refers to the extent which service met customers preferences and expectations (Haywood-Farmer, 1988). Supplies give customers tangible evidence to evaluate quality (Parasuraman et al., 1985). Service quality, however, depends on the customer's subjective evaluation of the service. The combination of expected service and the perceived service influence the perceived service quality (Parasuraman et al., 1985). The article "Service Quality: The Six Criteria of Good Perceived Service Quality" proposes criteria to answer this question (Gronroos, 1988). These criteria are divided into three categories: outcome-related criteria, process-related criteria, and image related criteria. These criteria include professionalism, attitudes, flexibility, reliability, recovery, and reputation. Based off the criteria, customers put the most emphasis on the process-related criteria (Gronroos, 1988). This likely is due to the nature of services which include customer input. In 2015, Hawkins et al. researched the way the acquisition process impacts the service quality. Their research found service quality is impacted by how adequately the definition of the requirement is defined by the customer. Also, the support and commitment from internal stakeholders increased the perceived service quality. The research conducted by Gronroos and Hawkins et al. demonstrates the importance of internal assessment even when evaluating an external organization. Based on these studies, internal factors affect how the quality of the service will be perceived. Finkenstadt (2020) studied specifically perceived service quality in knowledge-based services. His research supports the ideas presented by Gronroos and

Hawkins et al. Finkenstadt found perceived quality is multi-dimensional depending on the understanding of the customer, in addition to capability, dependability, and intelligent solutions provided by the firm's employees. Services present a unique challenge to acquisition professionals because of the complexity in measuring quality. Federal government acquisition specifically distinguishes service contracting from other acquisitions to address this variability.

c. Service Contracting

To acquire services, the federal government relies on contracts. The Federal Acquisition Regulation (FAR) governs how federal agencies award contracts to procure services to mitigate risk. FAR 37.101 (2022) defines a service contract as "a contract that directly engages the time and effort of a contractor whose primary purpose is to perform an identifiable task, rather than to furnish an end of supply." The FAR describes the policy contracting officers should use when dealing with service contracts. Specifically, the FAR urges contracting officers to use performance-based acquisitions to the maximum extent practicable. This reflects the unique nature of services regarding the intangibility (FAR 37.102, 2022). When drafting service contracts, agencies are asked to rely on performance work statements (PWS) rather than a statement of work (SOW) to describe the desired end result rather than restricting the contractor to a methodology (FAR 37.602, 2022). In other words, the government wants services performed to meet desired outcomes, but tries to avoid explaining how to perform them with the same level of detail that they might describe attributes of a product. The main types of contracts agencies use are fixed price contracts and cost-reimbursement contracts. Fixed price contracts transfer the liability to the contractor while the government absorbs the variable cost risk in a cost reimbursable contract. Typically, agencies strive to use fixed price contracts to control costs by locking in a total price and mitigate the risk of unexpected cost growth. To manage the taxonomy of goods and services, the DOD assigns Product Service Codes (PSC) to different types of services. There are nine broad service portfolio groups to categorize all service-related contracts (Assad, 2012):

- Research and Development
- Electronic and Communication Services
- Facility Related Services

- Knowledge Based Services
- Equipment Related Services
- Construction Services
- Logistic Management Services
- Medical Services
- Transportation Services (Assad, 2012, p. 2)

Service acquisitions typically require support from other functional areas leading to the creation of cross-functional project teams to manage service projects (Apte et al., 2010).

d. Services Specific Supply Chain Risks

The literature available regarding services specific supply chain risks shows how the relationship between the service provider and the customer influence the risk environment. The 2006 research conducted by Apte et al. examined the opportunities and challenges of managing the services supply chain within the DOD. They found the DOD's infrastructure for acquiring services is not as robust as the infrastructure for acquiring products and systems. They identify the need for the DOD to have knowledgeable clients to conduct sufficient surveillance and evaluate service quality. In 2010, Apte et al. continued their research and examined the differences between agencies in managing service acquisitions. Their recommendations include using fixed price contracts to obtain best value, increase the number of quality assurance evaluators, and increase the training of the acquisition workforce (Apte et al., 2010). Although this research was specific to the DOD, private industry can apply these recommendations to mitigate services supply chain risk. Although neither study examined the specific risk factors, both studies highlight how the characteristics and nature of acquiring services requires further research.

Several inputs factor into the quality performance of a service. The customer's perceived quality influences how they will rate the performance. Another factor is the complexity of the service. Complex service acquisitions are more vulnerable to performance risk because there are more opportunities for perceived quality shortcomings (Finkenstadt, 2020). In addition, narrow requirements threaten service performance because overly specific work statements restrict the service provider's ability to perform as intended (DiNapoli, 2021). This research demonstrates how customers can mitigate these service supply chain risks before engaging with providers. Because the services involve input from both the buyer

and the seller, both the buyer and the seller should be involved in risk mitigation and evaluation of risk factors. From the perspective of the provider, the customer introduces risk into their own supply chain and affect the provider's willingness to absorb financial risk (Selviardis & Norman, 2014). These risk factors include measurability of the service performance, the extent to which the relationship is transactional (as opposed to collaborative), and the balance of risks and rewards across the supply chain (Selviardis & Norman, 2014). Also, Selviardis & Norman found that the provider's ability to transfer risk to subcontractors increases their willingness to absorb financial risk.

e. Conclusion

The literature primarily discussed internal risk factors which could affect the service supply chain. The main risk factors identified include knowledgeable customers, existence of quality assurance evaluators, complexity of the service, the scope of the requirement of the service, and finally the extent to which the customer is involved in the service. The customer is the main influences over these risk factors. While this will be a consideration within the MITRE SoT, the literature did not discuss external risk factors which an organization should analyze when evaluating a provider. The goal of our research is to fill this gap within the literature.

3. Supply Chain Risk Management Techniques

Supply chain management involves managing the entire flow of goods, services, and information (Kamal & Irani, 2014). Effective management establishes control of the entire process to create a seamless flow of goods or services. It entails confronting risks and unforeseeable threats. Fortunately, there are existing methods, processes, and frameworks aimed at addressing supply chain risk management and mitigation. The Supply Chain Operations Reference (SCOR) model, the Triple-A Supply Chain, and Supply Chain Resilience Framework, are among the most well-known.

a. Supply Chain Operations Reference Model

The SCOR model, introduced by the Supply Chain Council, is a cross-functional framework for managing different levels of supply chain processes by dividing the supply

chain into five distinct components (Li et al., 2011). Li et al. (2011) describes these components as Plan, Source, Make, Deliver, and Return. They state managers should use the SCOR model within their own organizations and when communicating externally to standardize how managers discuss supply chains. Rizkya et al. (2019) also describes the SCOR model. They view the five components as the primary management processes to meet a customer's demand. Figure 2 depicts the structure of the SCOR model. It is not a linear process. The Plan component encapsulates each of the other components to show how planning should be incorporated into every aspect of supply chain management.

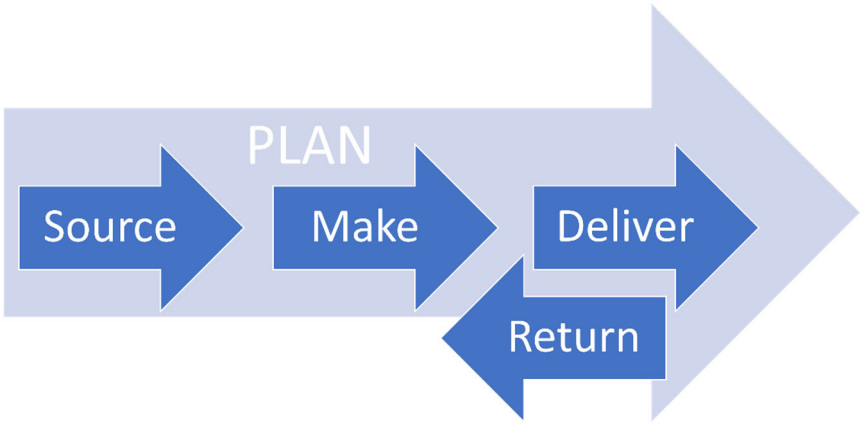


Figure 2. SCOR Model. Adapted from AIMS (2022).

b. Triple-A Supply Chain: Agility, Adaptability, and Alignment

The Triple-A supply chain (see Figure 3) highlights the importance of establishing agility, adaptability, and alignment in building effective supply chains (Lee, 2004). Agility empowers a supply chain to address short-term changes and disruptions quickly and efficiently in supply-demand variabilities in the market. Adaptability enables flexibility to modify processes and reinforces adjustments to longer, structural shifts in the market to make it more adaptive and future-ready. Lastly, through effective collaboration and information sharing with suppliers and customers, the alignment of objectives and incentives connects the entire supply chain to maximize performance and serve the end customer (Lee, 2004). The Triple-A concept remains vital to supply chain management in current and future business environments (Feizabadi et al., 2019).

There are countless scenarios for the fundamental application of the Triple-A concept. Recent disruptions, such as extreme drought, stress established supply chains and underline the need to be agile and pivot to respond to disruptions (Schiffling & Kanellos, 2022). Long-term shifts in the market connected to amplified globalization of supply and demand, new products being introduced at a faster pace, and quickened cycle times urge companies to enhance their organization's adaptability (Feizabadi et al., 2019). Alignment encourages firms to maximize incentives for all processes of the supply chain, thus improving performance and providing value for customers. Feizabadi et al. (2019) asserts that organizations who adopt the principles of Triple-A supply chain obtain a competitive advantage. For example, health services applying the Triple-A concept would be able to recognize a new disease and quickly find a way to treat the virus while maintaining medical service capacity to train doctors to treat the new threat. They also would incentivize suppliers to manufacture essential drugs needed for treatment. In this example, agility comes from being able to adjust to the new demand for services, adaptability stems from the flexibility to train new medical staff and they align their objectives by establishing incentives to their suppliers to respond to the new disease.

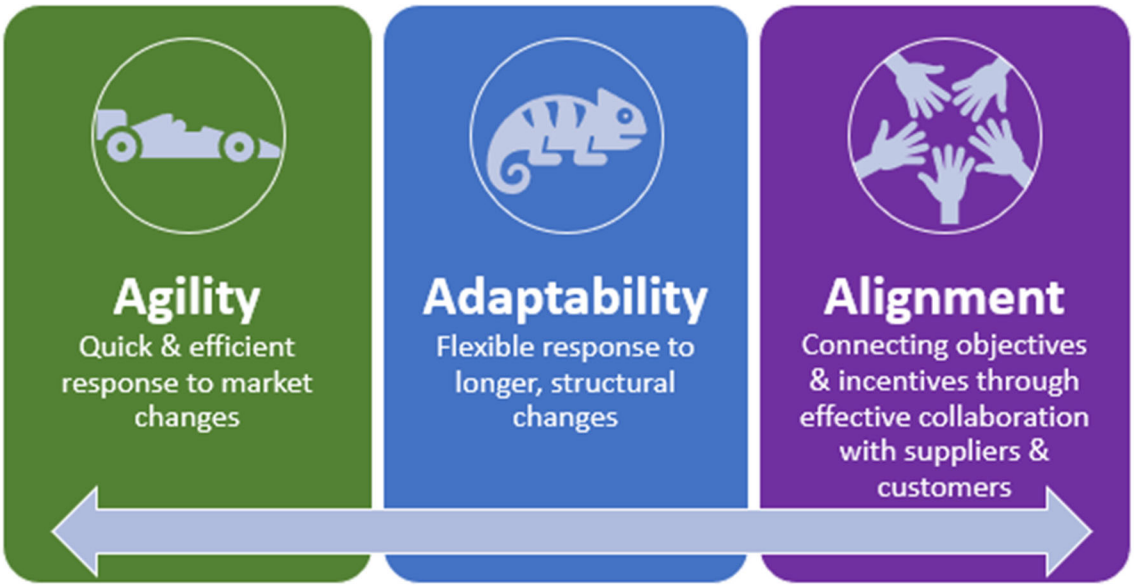


Figure 3. Triple A Supply Chain: Agility, Adaptability, Alignment. Adapted from Lee (2004)

c. Supply Chain Resilience Framework

Supply Chain Resilience (SCR) is a framework that compares the capabilities of a firm to respond to a disruption with the vulnerability or risk of a disruption (Shashi et al., 2020). This allows firms to intentionally design controls and establish reaction plans to restore their supply chains. Supply chains must be able to adapt promptly to internal and external risk events to retain profitability and keep their operations efficient and dynamic. We have demonstrated how massive disruptions are becoming more frequent and less predictable. Supply chains must be resilient to respond to unforeseen events. Managers should understand the potential risks facing their supply chain to effectively mitigate those risks (Aqlan & Lam, 2015). The authors of *Building the Resilient Supply Chain* asserted that supply chain resilience can be proactively engineered into a system through collaboration to identify risks, agility, and a culture of risk management (Christopher & Peck, 2004).

In readings and literature, characteristics of resilience are described as diverse, efficient, adaptable, and cohesive. The SCR Framework (Figure 4) was created as a tool for managers to measure the resilience of their organizations to assess and improve their processes (Pettit et al., 2010). Pettit et al. translated resilience concepts into the SCR Framework. With the development of a taxonomy, Pettit et al. was able to identify measurable vulnerability and capability subfactors for the first time. They stress the need to achieve a balance between vulnerabilities and capabilities. In a later paper, Pettit et al. (2019) notes that firms need to apply the SCR framework to every level of their supply chain and not just self-evaluate their capabilities and vulnerabilities.

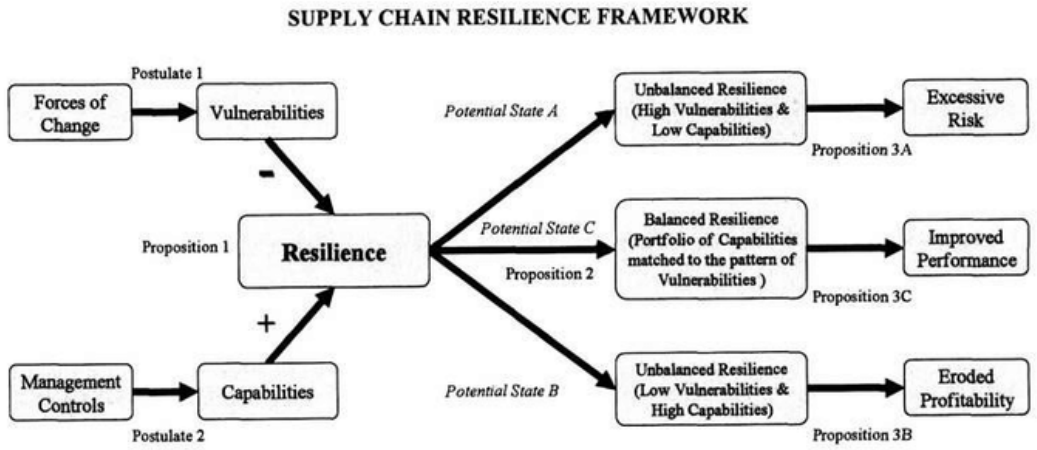


Figure 4. Supply Chain Resilience Framework. Source: Pettit et al. (2010).

d. Supply Chain Immunity

The COVID-19 pandemic revealed prevailing risk management techniques struggled to adapt in the face of massive supply chain disruptions. Resilient supply chains are no longer sufficient to respond to major interruptions (Handfield et al., 2022). An emerging supply chain risk management technique, supply chain immunity, is a nascent capability required to address future "slow-moving, persistent, and dispersed pandemics" (Handfield et al., 2022, p. 1). Handfield et al. offers four levels of preparedness to help an organization assess their immunity to disruptions (2021). The first level of preparedness is reactive, insinuating a lack of awareness. The second level, responsive, still lacks complete awareness, but has more capability to respond to emergencies. Third, resilience, maintains robust awareness but struggles to mobilize resources quickly. Finally, the apogee of the four levels, immunity, refers to a supply chain with redundancies and the ability to quickly mobilize and respond to a massive disruption. This requires redundant networks and an understanding of the nodes of the supply chain. To move from a resilient supply chain to an immune supply chain, organizations need transparent communication amongst external organizations regarding shortages, and to share supplies of critical goods (Handfield et al., 2021). Organizations should not wait for a shortage to respond to a disaster. Their supply chains need to be actively managed to meet demands, especially in the face of a public health crisis (Handfield et al., 2020)

4. Conclusion

Supply chain risk management aims to reduce the probability of risks occurring and to bolster the response to realized threats while minimizing their impact (Pujawan & Geraldin, 2009). Ostensibly, the methods and frameworks in place develop resilience and offer dynamic flexibility to managers giving the idea of control. However, the emerging challenges seen with increased interruptions to the global supply chain highlight weaknesses with these models. In their peer-review journal article titled "Supply Chain 2.0: Managing Supply Chains in the Era of Turbulence," Christopher & Holweg (2011) argue that current supply chain risk management theories do not consider an environment prone to disruptions. They also state that in order to succeed in an era of uncertainty and ever-changing business environments, there is a need for structural resilience that incorporates flexible options into the supply chain design. The novel supply chain immunity concept addresses these concerns by incorporating adaptability into the resilience model of supply chains (Handfield et al., 2022. Supply chain security seeks to minimize security risks while ensuring an efficient flow of goods and services from suppliers to customers (Tong et al., 2022). The problem is not novel, but continued research is needed to address gaps in literature. The supply aspect of supply chains does not address the intangibility of services. Service also involves co-development with customers, a feature not scrutinized when evaluating the risk factors associated with supplies. Our research attempts to fill knowledge gaps focused on the identification of risk factors and utilization of that knowledge to make better business decisions.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

This chapter provides an overview of the methodology used within our study. Our research methodology included a data collection phase and a data analysis phase. We relied on interviews with acquisition and contracting professionals within the DOD to collect data. We conducted semi-structured interviews to enable an exploratory research approach and developed questions to guide our discussions. The participants included program managers and contracting officers at various organizations within the DOD. We then applied thematic analysis to evaluate our qualitative data (Creswell & Poth, 2018). This included organizing interview data, labeling key words, identifying patterns, and interpreting the results.

A. DATA COLLECTION

We collected qualitative data derived from nine interviews conducted over the course of six weeks. We based interview questions on MITRE's SoT to explore supply chain risks relating to MITRE's four defined risk areas. The interviewees represented acquisition organizations within the DOD as current and prior contracting officers or program managers.

1. Interview Design

We relied on semi-structured interviews for the exploratory parts of our research. We needed to be able to delve deeply into certain topics and ensure we understood the responses. Semi-structured interviews best enable open-ended and free flowing conversation to take place (Harrell & Bradley, 2009). Semi-structured interviews consist of an open-ended dialogue, guided by an outline, and includes probing questions or comments (DeJonckheere & Vaughn, 2019). We sought to elicit discussion with our interviewees to understand their organizations' best practices for dealing with supply chain risk, especially those risks particular to services. The length of the interviews ranged between 45 minutes and 90 minutes. We conducted interviews virtually using Microsoft Teams and Zoom.gov. For each interview, we designated one interviewer and one note taker. The note taker was permitted to ask clarifying questions at any time. At the beginning of each interview, we instructed our interviewees to strictly discuss their organization's policies and practices relating to supply

chain risk management. We avoided any subjective opinions regarding organization's policies and practices.

2. Question Design

When conducting semi-structured interviews, the questions serve as a roadmap for discussion and can be re-worked or tailored dependent on the situation throughout the research process (Adams, 2015). Our outline consisted of nine questions, with four related to the SoT risk areas, (listed below) intentionally designed to start very broadly and gradually target specific topic areas.

1. What types of services does your organization procure?
2. What supply chain risks related to services does your organization experience?
3. What does your organization identify to be the risk factors affecting the services' security?
4. What does your organization identify to be the risk factors affecting the services' reliability?
5. What does your organization identify to be the risk factors affecting the services' quality?
6. What does your organization identify to be the risk factors affecting the services' integrity?
7. What are the indicators of these risks within your organization (red flag indicators)?
8. How does your organization mitigate/prevent/respond to these risks?
9. How does your organization collect data on supply chain risk factors?

We started each conversation around services and challenges regarding services when dealing with the supply chain. Then we moved from those discussions to a conversation

regarding risk factors, risk indicators, and risk management techniques. We broke the third question regarding risk factors into four different parts to link to MITRE's current SoT model. Within the SoT, MITRE identified four risk areas within the services category, under which they planned to assign risk factors and subfactors (Ref Section SoT Risk Areas for more info regarding the specific risk areas.)

3. Participant Selection

Our participants (listed in Table 3) included current and prior acquisition and contracting professionals within the DOD. They represented the following organizations: Naval Air Systems Command (NAVAIR), Air Force Life Cycle Management Center (AFLCMC), Air Force Installation Contracting Center (AFICC), Air Combat Command (ACC), Acquisition Management and Integration Center (AMIC), Defense Logistics Agency (DLA), and Headquarters Air Force (HAF). These organizations procure services including but not limited to professional services, knowledge-based services (KBS), software as a service (SaaS), logistics services, and research and development services. We did not restrict our interviews to only one participant. Two interviews involved a group of individuals from a program office with different roles. For example, our interview with ACC AMIC regarding the Internet-Based Contractor Operated Parts Store (ICOPARS), involved both the program manager and members from the contracting office. The same was true for the Combat Air Forces/Contracted Air Support (CAF/CAS) program also within ACC AMIC. Table 3 depicts whether the interview focused on general services or a specific program.

Table 3. Interview Participants

Date	Organization/ Office	Name	Role	Services Discussed
15 Jul 22	NAVAIR*	CDR Michael Schilling	Contracting Officer*	General Services
22 Jul 22	AFLCMC*	Dr. Rene G. Rendon	Contracting Officer*	General Services
12 Aug 22	AFICC	Lt Col Daniel Stephens	Enterprise Sourcing Squadron Commander	General Services
17 Aug 22	AFLCMC	Peter Lee	Logistics Manager	Enterprise Information Technology as a Service (EITaaS)
18 Aug 22	ACC AMIC	Kevin Kleinhenz Jeff Park MSgt Peter Mwangi	Services Acquisition Program Manager AMIC Vehicle and Age Functional Vehicle Manager	Internet-Based Contractor Operated Parts Store (ICOPARS)
19 Aug 22	ACC AMIC	Joshua Hudson Jeremy Young	Program Manager Contracting Officer	Combat Air Forces/ Contracted Air Support (CAF/CAS)
29 Aug 22	AFPEO/CM	MaryKathryn Robinson	Strategic Sourcing Chief	General Services
29 Aug 22	DLA	Cathy Contreras	Acquisition Executive	General Services
09 Sep 22	DLA	Joseph Marquis	Contracting Officer	General Services

*Denotes relevant prior organizational experience. These interviewees no longer served in those organizations.

B. DATA ANALYSIS

For the purpose of this research, we conducted a thematic analysis from exploratory interviews. Thematic analysis is a method used to extract themes from qualitative data (Creswell & Poth, 2018). As aforementioned, there is a gap in the literature regarding service specific supply chain risk factors. Therefore, we decided exploratory research was the most appropriate research method. Researchers recognize thematic analysis for its flexibility and ability to identify patterns in a large amount of qualitative data (Braun & Clarke, 2006). This refers to its ability to present data in a way easily understood outside of academia. Thematic analysis involves six phases (Braun & Clarke, 2006) (ref Table 4).

Table 4. Phases of Thematic Analysis.
Adapted from Braun and Clarke (2006).

Phase	Description of the Process
Data Familiarization	Review interview data and note initial ideas
Generate Initial Codes	Code features of the data across the entire interview
Identify Themes	Collate codes into potential themes
Review Themes	Check if themes work in relation to the coded extracts. Generate a thematic map of the analysis
Define/Name Themes	Conduct ongoing analysis to refine each theme
Produce the Report	Final analysis: extract examples relating back to research questions and literature and produce a scholarly report

We recorded the data collected from our interviews via Microsoft Teams or Zoom.gov. Upon completion of interviews, transcribed data was subjected to thematic analysis. We identified themes within our interview notes for each question. We began organizing and synthesizing our data on a single worksheet to easily identify themes and patterns. Once reaching saturation, we stopped data collection and shifted to reviewing the themes. Saturation refers to information redundancy at which no new themes develop from additional interviews or data collection (Braun & Clarke, 2019). Our method of determining saturation involved ongoing data analysis. For our study, saturation means the point at which further interviews do not yield new information relevant to our research questions (Guest et al., 2020). We identified the main themes after our first six interviews. Our final three interviews did not reveal any new themes; therefore, we ended our data collection phase. Guest et al. found six to seven interviews resulted in 80% of saturation (2020). This puts our nine interviews in line with the amount generally required to reach saturation. These themes reveal the indicators of supply chain risks unique to DOD services. They also portray the best practices utilized by procurement professionals for mitigating DOD service specific supply chain risks.

To perform the analysis, we developed codes relevant to the corresponding interview questions for each interviewee. Then we systematically organized the codes into themes and

counted how many times the code appeared in our data using Microsoft Excel. Each row in our table corresponded to a unique code. We counted the number of coding references under each theme to analyze the frequency of each theme in our data. We also labeled each theme as either service specific or generic to each part of the supply chain (i.e., services, supplies, and suppliers). Themes we deemed generic should still be considered relevant risks to the service aspect of the supply chain. From this data table, we filtered by the type of theme, which corresponded to an interview question, and yielded a working model for supply chain risks relevant to the services aspect. Figure 5 provides a visual representation of our process for generating codes and themes. A code is a subcomponent of a theme. For example, inflation and unemployment are codes we identified. The overarching theme for these codes is economic risk factors.

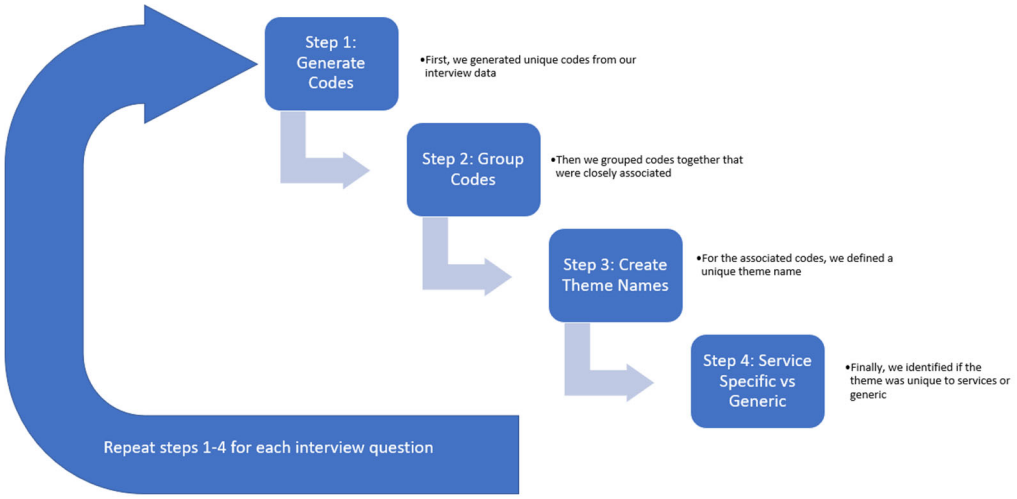


Figure 5. Thematic Analysis Methodology

C. CONCLUSION

In this chapter, we identified our methodology used in the study. Additionally, we discussed how this qualitative methodology helped survey the supply chain risks experienced by various DOD organizations. This chapter also described how we selected our participants, collected data, and analyzed responses. In the next chapter, we present the results of our study.

IV. RESULTS/DISCUSSION

In this chapter, we discuss the results of our thematic analysis that create the foundation of our Services Supply Chain Risk Management Framework (Appendix C). Our initial research and exploration determined there is a gap in literature regarding service specific supply chain risk factors. Our data revealed a host of influencing risk factors that affect the services aspect of a supply chain. Furthermore, this chapter will discuss the SoT's four defined risk areas (security, reliability, quality, and integrity) and identify the risk factors affecting each risk area. Additionally, we examine risk indicators, risk mitigation techniques, and data available to supply chain managers. Then we identify the risk factors experienced most frequently by the organizations we interviewed. Finally, we apply our framework to ICOPARS, a DOD supply chain for vehicle parts, to demonstrate the application of our results.

A. SUPPLY CHAIN RISK FACTORS

The data in this section was derived from the responses to the four interview questions we asked our interviewees regarding risk factors affecting each of the four SoT risk areas, questions 3a- 3d. We identified themes related to risk factors within each SoT risk area. However, we found overlapping risk factor themes across the SoT risk areas. Table 5 shows all the unique risk factor themes we identified across the four risk areas. In the table, each theme breaks down to show the associated codes for each respective theme. For example, we grouped together the codes *cyber, information leakage,* and *origin of supplies* and generated the theme name: *Counterintelligence (CI) Risk Factors.* The values in the table represent the frequency of each code across the interviewees. We counted each time an interviewee referenced the code. We did not double count if an interviewee referenced the code twice in the same interview while discussing the same question. If an interviewee referenced a code when answering a question about security and then again when responding to a separate question regarding quality, we counted the code for each respective risk area. We provide definitions for all the supply chain risk factors in Appendix D.

Table 5. All Risk Factor Themes and Relevant Codes

Services Supply Chain Risk Factors	Integrity Risk Factors	Quality Risk Factors	Reliability Risk Factors	Security Risk Factors	Grand Total
Availability Risk Factors			**2**		**2**
Service Availability			2		2
Bureaucratic Risk Factors		**1**	**1**	**1**	**3**
External approvals to perform service		1			1
International Laws				1	1
International Shipping Restrictions			1		1
CI Risk Factors				**5**	**5**
Cyber				3	3
Information Leakage				1	1
Origin of Supplies				1	1
Contract Administration Risk Factors	**1**	**2**			**3**
COR Training		2			2
Qualified oversight officials	1				1
Contract Structure Risk Factors			**2**	**3**	**5**
Excessive Security Requirements				2	2
Supply Chain and Contracting Chain Alignment			2	1	3
Contractor Experience Risk Factors		**1**			**1**
Evaluating relevant past performance		1			1
Customer Risk Factors	**2**	**3**			**5**
Customer Education		1			1
Customer Relationship with Service Provider	1	1			2
Customer Satisfaction	1	1			2
Economic Risk Factors	**2**		**1**		**3**
Inflation	1		1		2
Unemployment	1				1
Personnel Risk Factors	**1**	**4**	**1**	**4**	**10**
Number of Parties Involved				2	2
Personnel Turnover		1			1
Qualified Personnel	1	3	1		5
Reliance on KTRs to Address Security Issues				2	2

Services Supply Chain Risk Factors	Integrity Risk Factors	Quality Risk Factors	Reliability Risk Factors	Security Risk Factors	Grand Total
Requirement Generation Risk Factors	**3**	**2**			**5**
Opaque Requirements	3	2			5
Supporting Infrastructure Risk Factors	**2**	**3**	**6**		**11**
Availability of supporting systems	1				1
Company Capacity			4		4
Reliance on third parties to support service	1				1
Service Enabling Supplies		3	2		5
Grand Total	**11**	**16**	**13**	**13**	**53**

1. Security Risk Factors

The data from this section relates to the interview question "What does your organization identify to be the risk factors affecting the services' security?" We identified four unique themes within the security risk area. These include bureaucratic risk factors, contract structure risk factors, personnel risk factors and CI risk factors. Figure 6 shows the frequency with which each theme arose during our data collection.

Figure 6. Security Risk Factors Model Data

CI risk factors was the most common theme identified. This risk factor includes concerns about information leakage, cyber security concerns, and origin of supplies. The nature of the requirement dictated the security requirement for the service provider. Although CI risk factors represent an important concern when dealing with services, especially professional and cyber related services, this risk factor is generic to each aspect of the supply chain: supplies, suppliers, and services. The second most prevalent theme, personnel risk factors, includes risks associated to the number of parties involved in a service. Security risks compound as more parties and layers of subcontractors are needed to perform a service. Another subfactor within personnel risk factors includes the reliance on contractors to address customer's security concerns. Customers may need to rely on a service provider's technical expertise to address security concerns, however this increases the security risk. Contract structure risk factors was the third most common theme we identified under security. One concern included extraneous security requirements. Over-burdening the service with ambiguous or unneeded classification requirements limits the pool of potential suppliers. Furthermore, the contract structure risk factors include the alignment between the supply chain and the contracting chain. The contracting chain refers to the network of contractors and subcontractors interacting for a program or project and how they communicate with the contracting officer and the contracting officer representative (COR). Alignment comes from aligning the customer-vendor relationships with the management of the supply chain. These risk factors also include risks of bridge contracts and risks of losing parties protesting. Finally, bureaucratic risk factors refer to laws and restrictions governing the performance of a service, especially when conducting business internationally.

2. Reliability Risk Factors

The data in this section relate to the interview question "What does your organization identify to be the risk factors affecting the services' reliability?" We identified six unique themes related to the reliability of a service as shown in Figure 7. Some of these themes overlap with the themes previously identified relating to security risk factors. We found interviewees considered some of the risk factors relevant to more than one risk area.

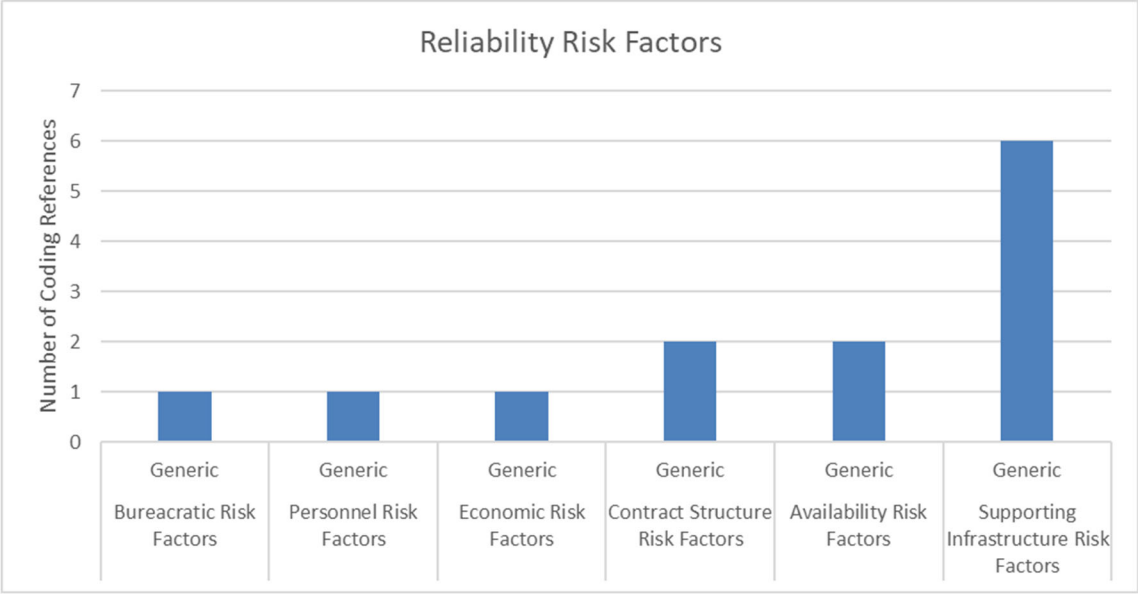


Figure 7. Reliability Risk Factors Model Data

Supporting infrastructure risk factors was the most prevalent theme related to reliability. We labeled this theme to capture the risks to a service because of the underlying goods needed to perform the service. Also, a company's capacity carries risk we consider to be part of the supporting infrastructure. Next, availability risk factors refers to the availability of the necessary service. Some requirements may be too specific, and no available services exist to meet the requirement. Contract structure risk factors again refers to the alignment between the supply chain and the vendor management chain. As discussed under security risk factors, mis-aligned chains and decentralized control when coordinating multiple service efforts dampers communication and threatens the performance of the service and the over-arching supply chain. Economic risk factors include external economic conditions that may impede the service's performance. Inflationary pressures and high unemployment rates contribute to this risk factor. Personnel risk factors refers to personnel with the necessary qualifications to meet the requirements of a service. Finally, bureaucratic risk factors refers to any barriers in place because of laws and regulations impeding the performance of a service.

3. Quality Risk Factors

The data in this section relates to the interview question "What does your organization identify to be the risk factors affecting the services' quality?" Within the quality risk area, we identified seven risk factor themes. Some of the risk factors identified affecting a service's quality, also affect a service's reliability. We anticipated this based on the SoT definition of reliability i.e., the ability of a service to provide quality over time. Also, research shows reliability (involving consistency of performance and dependability) is one determinant of service quality (Parasuraman et al., 1985) Figure 8 displays the themes we identified as well as the number of coding references for each theme within our data.

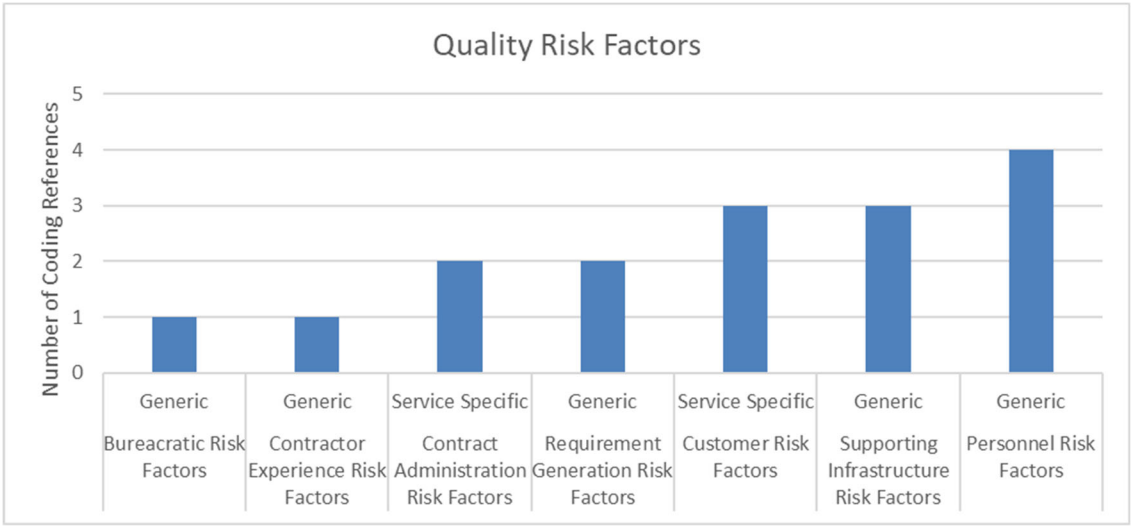


Figure 8. Quality Risk Factor Model Data

Personnel risk factors was the most prevalent theme related to quality. This includes the presence of qualified personnel to accomplish the service as well as personnel turnover which could affect the service quality. Supporting infrastructure risk factors tied with customer risk factors as the second most prevalent theme. We also identified supporting infrastructure risk factors affecting the reliability of a service. Next, we identified the customer risk factors theme to be unique to services because it includes customer education and customer relationship with the provider. A distinguishing characteristic of services is

the input from both the customer and the provider (Apte et al., 2006). Because of this characteristic, the customer also presents a risk to the services aspect of the supply chain. The customer's perceived quality is influenced by the education level of the customer. This finding is supported by the research conducted by Finkenstadt into perceived service quality within knowledge-based services (2020). Finkenstadt found the customer's understanding and training level influences the perceived service quality.

Requirement generation risk factors refers to opaque requirements negatively impacting the quality of a service. This shows the importance of assessing risk internal to an organization as well as external to the organization. The other risk factor we identified to be unique to services was contract administration risk factors. This refers to the oversight of the performance of a service. Within the DOD, contract administration is typically a function of Contracting Officer Representatives (CORs). Untrained or inexperienced oversight officials creates risk to services. We considered this service specific because administration and oversight become necessary due to the complexity of the measurement of services, as well as the intangibility of the output. Next, contractor experience risk factors refer to the experience of the service provider. In assessing an offeror, managers need to evaluate relevant performance history to ensure the offeror can fully meet the requirement. Finally, bureaucratic risk factors re-appeared while discussing quality. Similar to the bureaucratic risk factors affecting reliability, different laws and regulations could impede the performance of a service. Bureaucratic risk factors also include environmental rules and regulations, such as National Environmental Protection Act requirements for construction contracts.

4. Integrity Risk Factors

The data in this section relates to interview question "What does your organization identify to be the risk factors affecting the services' integrity?" Within the integrity risk area, we identified six risk factor themes. The SoT considered integrity as the extent to which something remains complete, unmodified, unimpaired, and uncorrupted from its intended form (M. Ripley, personal communication, August 1, 2022). Our interviewees struggled with this definition as the other three risk areas seem to encapsulate integrity.

That is, if a service can be characterized to be reliable, of acceptable quality, and secure, it will automatically have integrity. All the themes captured within the integrity risk area overlap with themes identified in the other risk areas. We did not identify any risk factors unique to integrity. Figure 9 displays the themes we identified as well as the number of coding references associated with each theme.

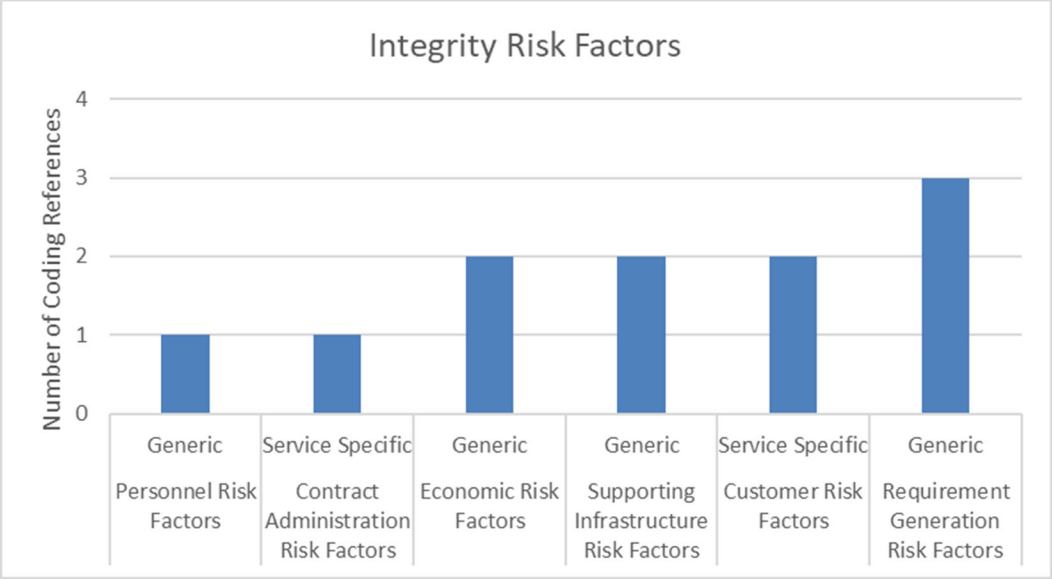


Figure 9. Integrity Risk Factor Model Data

As a result, our data supports the interviewees' observations that the SoT definition of integrity encapsulates the definitions of reliability, quality, and security.

5. Combined Risk Factors

Many of the risk factors overlapped across preestablished SoT risk areas. Figure 10 provides a visual to demonstrate this overlap across the different risk areas. This graph shows that managers identified two risk factors most affecting their services. These include supporting infrastructure risk factors and personnel risk factors. From this we conclude these two risk factors should be the primary concerns of supply chain risk managers. The personnel performing the service and the tools or supplies the personnel require are the most prevalent supply chain risk.

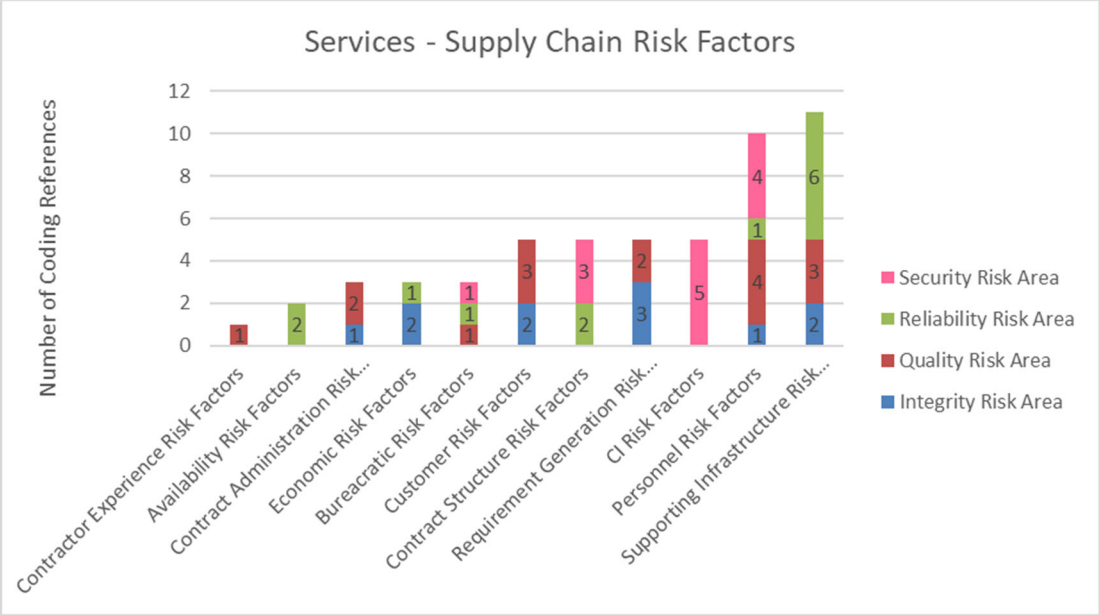


Figure 10. Overlapping Risk Factors

Figure 10 also illustrates how the risk areas we identified overlap. We identified only three risk factors that were unique to one specific area. CI risk factors were unique to the security risk area. Contractor experience risk factors and availability risk factors were also unique to the quality and reliability risk area respectively. However, these risk factors were the least prevalent in our data. The two risk areas with the most overlap were quality and integrity. With only the exception of bureaucratic risk factors, each risk factor identified within the integrity risk area was also identified in the quality risk area.

B. RISK INDICATORS

The data in this section relates to the interview question "What are the indicators of these risks within your organization?" Risk indicators serve as a warning tool or a red flag signaling to organizations that there is a potential vulnerability and a risk could occur. These indicators tell managers a problem exists or there is a presence of a risk factor. The risk indicators derived from our interview data are portrayed in Figure 11. The most common risk indicator identified was service performance metrics such as past performance and if a contractor met the quality assurance surveillance plan (QASP). Most interviewees stated they use Contractor Performance Assessment Reports (CPARS) to

evaluate past performance. Measurements such as schedule and performance were also grouped into the service performance metric category. This entails data reflecting the timeliness and past performance of a contractor. Interviewees stated that they were able to identify red flags through monitoring of the contract and recognizing incidences when the contractors' actual performance was not aligned with the planned contract. Additionally, risk indicators were identified through customer feedback (i.e., customer reports or feedback from the COR). Cost metrics and external factors were also numerously identified as risk indicators. The cost metric indicator refers to costs exceeding expected rates or budgeted funds, thus impacting the outcome of the service. External indicators were referenced as circumstances such as geopolitical unrest, economic issues, environmental incidences, international customs, etc.

Further risk indicators identified were personnel issues (e.g., labor issues and workforce availability) and procurement fraud. By identifying risk indicators, organizations are better equipped to take resilient measures to support the services aspect of the supply chain. Gaudenzi & Borghesi (2006) recognize the importance of identifying risk indicators and quantifying their potential impact to the organization in order to build resilient supply chains.

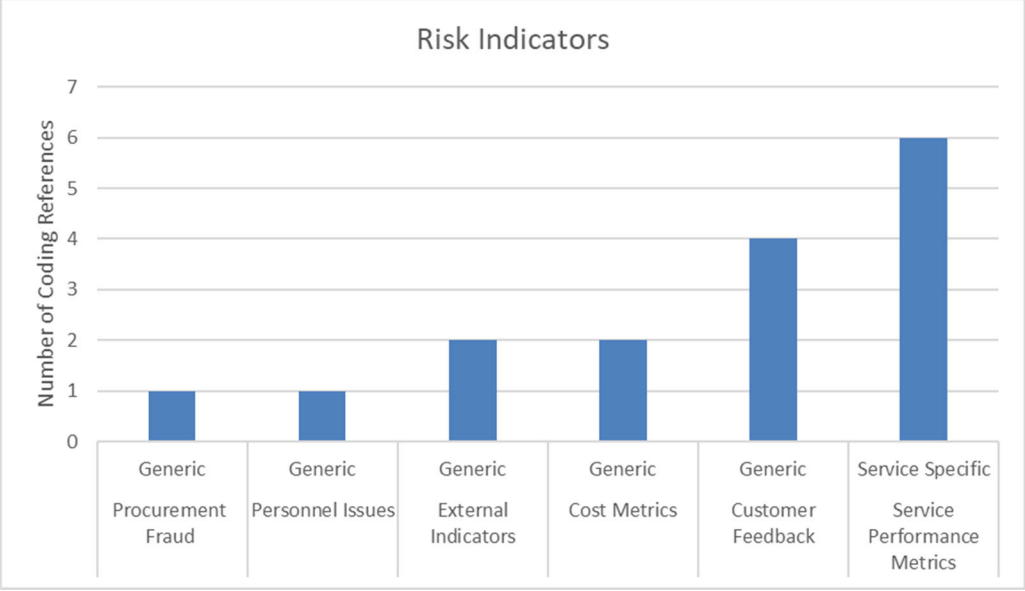


Figure 11. Risk Indicators

C. MANAGING RISK

In addition to identifying supply chain risks and their indicators, we identified best practices acquisition managers use to mitigate those risks and also data available to managers making decisions. The mitigation techniques we identified from our interviews reinforce how the DOD teaches managers to mitigate risk.

1. Mitigation Techniques

The data in this section corresponds to the interview question "How does your organization mitigate/prevent/respond to these risks?" The codes from the interview data offer four overarching best practices to mitigating supply chain risks. Figure 12 shows these themes and their frequency from our interviews.

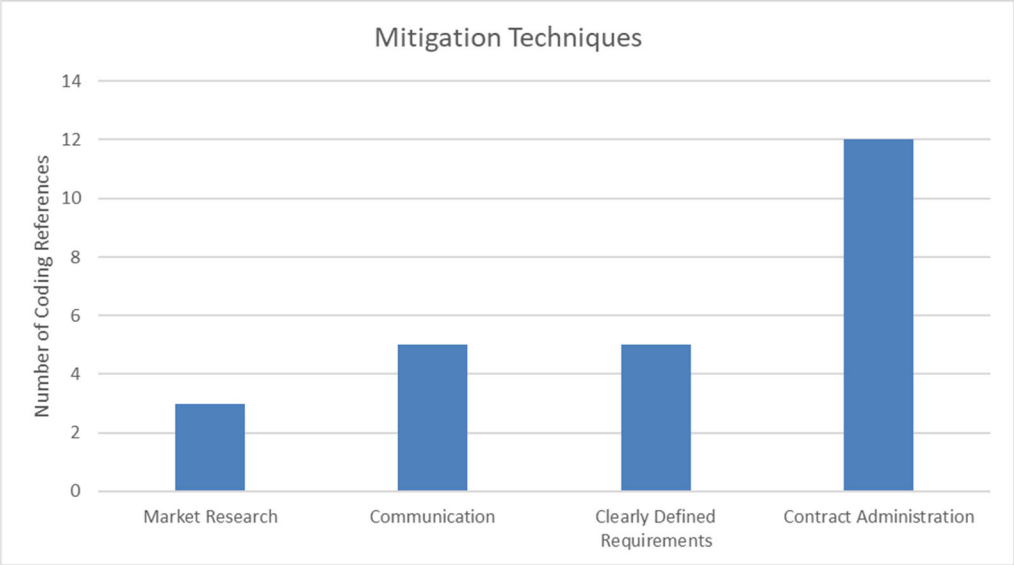


Figure 12. Mitigation Technique Model

The mitigation techniques we identified likely suffer from confirmation bias. Our pool of interviewees consisted of DOD acquisition professionals. The mitigation techniques they described all are part of an acquisition plan during the planning phase of a contract award (FAR 7.105, 2022). As a result, none of our themes are nascent, but instead validate the importance of planning in supply chain risk management.

2. Data Collected

The results in this section correspond to the interview question "How does your organization collect data on supply chain risk factors?" We found organizations within the DOD collected minimal data regarding supply chain risks. From our interviews, we identified three types of data routinely collected to help manage a supply chain: economic data, intraorganizational data, and past performance data. Table 6 shows the themes we identified and the corresponding codes.

Table 6. Supply Chain Risk Data

Data Collected	Number of Coding References
Economic Data	**2**
Bankruptcy Data	1
Unemployment Rates	1
Intra-Organization Data	**7**
Customer Feedback	3
Performance Metrics/Thresholds	4
Past Performance Data	**5**
CPARS	5

Some organizations collect economic data to assess not only organizations, but also the environment in which they were conducting business. For example, managers may track currency rates when conducting business internationally. Bankruptcy data serves to identify financial weaknesses within an organization. Unemployment rates, however, measure the economic environment. These rates reveal labor issues in foreign markets and are a consideration managers use to manage their supply chain. Organizations also collect intra-organizational data throughout the period of performance. This data usually relates to the pre-defined performance metrics. These organizations also track customer feedback.

Feedback and performance monitoring are not unique to the services aspect of the supply chain; however, these metrics may be more difficult to define because of services' intangibility and heterogeneity characteristics. This type of data cannot assess an organization prior to establishing a relationship and is used to monitor risk throughout the performance. Finally, contracting officers and program managers use CPARS to communicate feedback inter-agency regarding contractor past performance.

D. REALIZED SUPPLY CHAIN RISKS

In this section we quantify supply chain risks our interviewees experienced. This data comes from responses associated to the interview question "What supply chain risks related to services does your organization experience?" We generated new codes from the responses; however, we assigned the codes to the risk factor themes we previously identified in Section A. We did not generate new theme names for associated codes. This highlights the risks our interviewed organizations historically have experienced. Table 7 shows these themes along with the relevant codes and their frequency. The number of coding references represents the number of times an interviewed organization experienced the risk. The codes with the most frequent occurrences were qualified personnel (5) and manufacturing/ capacity issues (3). Interviewees noted their organizations struggled to obtain qualified personnel to provide a given service. For example, offerors may bid on an award and provide resumes of personnel they expect to hire to perform the service. When it comes time to perform the service, the actual personnel hired may differ. Interviewees also struggled with manufacturing and capacity issues. The COVID-19 pandemic revealed manufacturing weaknesses in supply chains. However, interviewees also noted some smaller businesses struggled to provide the capacity for services on larger projects.

Table 7. Experienced Supply Chain Risks

Services Supply Chain Risk Factors	Number of Coding References
CI Risk Factors	**1**
Foreign Adversary	1
Contract Administration Risk Factors	**2**
Poor Oversight	2
Contract Structure Risk Factors	**2**
Bridge Contract Risk	1
Protest Risk	1
Contractor Experience Risk Factors	**1**
Relevant Past Performance	1
Economic Risk Factors	**3**
Cost Control	2
Inflation	1
Personnel Risk Factors	**9**
Contractor Timeliness	2
Qualified Personnel	5
Subcontractor Tiers Maintaining Continuity	1
Contractor Performance	1
Requirement Generation Risk Factors	**1**
Opaque Requirements	1
Supporting Infrastructure Risk Factors	**6**
Component Capability	1
Lead Times	1
Manufacturing/Capacity Issues	3

Services Supply Chain Risk Factors	Number of Coding References
Website Uptime Verse Downtime	1
Customer Risk Factor	**2**
Customer Satisfaction	2
Bureaucratic Risk Factors	**2**
Environmental	1
Geopolitical	1

Figure 13 highlights that the risks most frequently experienced by our interviewees were related to personnel risk factors and supporting infrastructure risk factors. This suggests that within the DOD, problems arise most frequently with obtaining qualified personnel and ensuring the personnel have the materials and capacity to perform a service. The two service specific risk factors were customer risk factors and contract administration risk factors. These are unique to services because of the heterogeneity of services. Supplies can be easily standardized, alleviating these risks. Services, however, are more complex and involve customer input which elevate the risks associated with customer risk factors and contract administration risk factors.

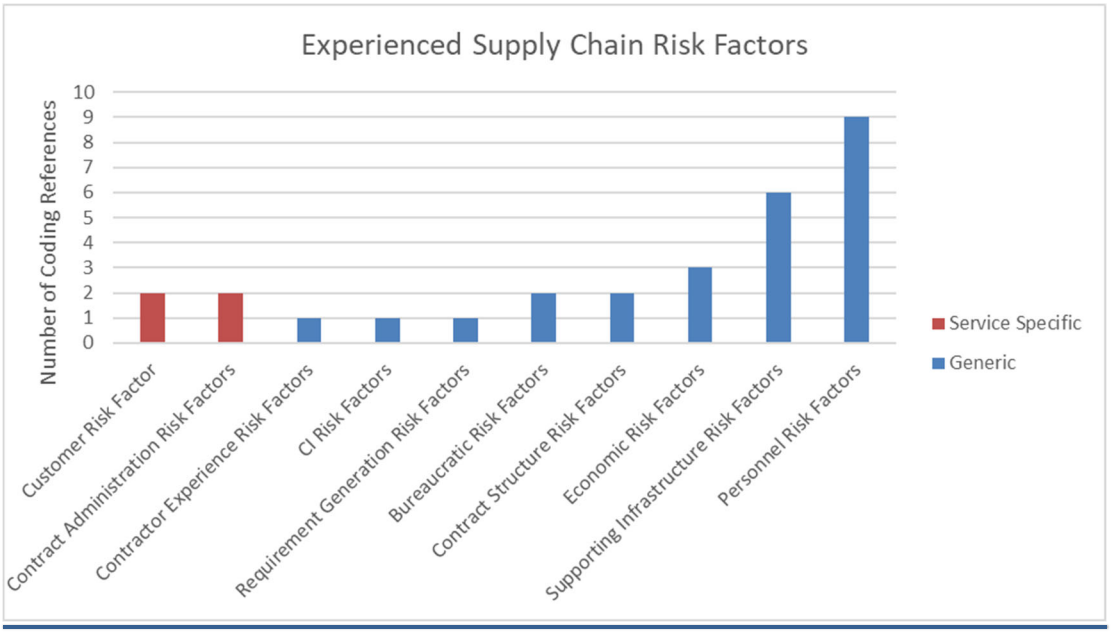


Figure 13. Frequency of Experienced Supply Chain Risk Factors

E. ICOPARS

The ICOPARS program provides an example of a DOD supply chain and the risks associated with the service aspect of the supply chain. The ICOPARS program managers noted ICOPARS is not categorized as service contract. This Indefinite Delivery Indefinite Quantity (IDIQ) supplies contract provides vehicle parts to support military members operating in the U.S. Air Forces Central (AFCENT) area of operations including Southwest Asia and Africa. Although the program provides supplies, the program contains service components which support the supply chain. The actual maintenance is performed by the service members in country. The supply chain relies on the logistics service to deliver the parts to the members overseas. Also, ICOPARs provides an online storefront to the members to easily order parts. This front-end system establishes parts requisition. The program managers consolidated the program under one vendor. The vendor maintains the online storefront and then resources the parts needed and coordinates shipping.

We can apply the risk factors we identified to ICOPARS to demonstrate their impact on the supply chain for vehicle parts. Table 8 shows the supply chain risks we identified and examples of how they are manifested in the ICOPARS program.

Table 8. ICOPARS Services Supply Chain Risks

Services Supply Chain Risk Factors	ICOPARS Specific Risks
Contractor Experience Risk Factors	The contractor needs to have experience managing the volume of orders required for the contract
Availability Risk Factors	The contractor needs to ensure they identify a vendor who is able to ship car parts overseas
Contract Administration Risk Factors	Poor oversight of the contractor threatens the service's dependability
Economic Risk Factors	Increases in oil prices affects shipping costs
Bureaucratic Risk Factors	International laws may threaten the ability to ship parts overseas
Customer Risk Factors	Unsatisfied customers will not use the service
Contract Structure Risk Factors	Aggressive performance incentives in the contract risk incentivizing fraudulent behavior
Requirement Generation Risk Factors	Vague/ unclear parts specifications may result in incompatible parts being delivered
CI Risk Factors	The online store front needs to be secure from any cyber attacks
Personnel Risk Factors	Relying on a subcontractor for shipping the parts adds risk because the government does not have privity with the subcontractor. This introduces another party to the supply chain.
Supporting Infrastructure Risk Factors	The website needs to have capacity to support a certain number of customers or users

To manage these risks, the managers collect qualitative and quantitative data throughout the performance of the contract. Qualitative data, such as customer feedback, measures the quality of the online storefront. Quantitative data, such as website uptime versus downtime and lead times for parts, measures the reliability of the services involved in the supply chain. Table 9 shows our risk indicator framework and how it applies to ICOPARS.

Table 9. ICOPARS Risk Indicators

Risk Indicators	ICOPARS Specific Risk Indicators
Procurement Fraud	Procurement fraud red flags such as duplicate invoices for parts
Personnel Issues	High levels of personnel turnover
External Indicators	High inflation / high unemployment
Cost Metrics	Exceeding cost targets or budgeted costs
Customer Feedback	Customer feedback suggesting issues with online storefront
Service Performance Metrics	Longer than expected lead times for parts

The supply chain risks and risk indicators associated with ICOPARS shows how our research can be applied to the service aspect of supply chains. Although not all the risks are unique to services, how they apply to the services aspect may differ from how they apply to the supplies or supplier aspects.

F. CONCLUSION

In this section, we presented the results of our research and outlined our framework for considering services related supply chain risks. Also, we identified risk factors associated to each risk area within the SoT. We then discussed risk indicators and mitigation techniques managers use to manage their supply chain risks. Finally, we apply our research to a DOD supply chain for vehicle parts to demonstrate its application. In the next section, we answer our research questions, provide recommendations to MITRE regarding the SoT, introduce our Services Supply Chain Risk Management Framework, and discuss the limitations of our study and areas for future research.

V. CONCLUSIONS AND RECOMMENDATIONS

A. RESEARCH QUESTIONS ANSWERED

This research aimed to answer two questions regarding the services risk factors, as well as identifying techniques and best practices to mitigate risk unique to services. Additionally, in this final chapter, we outline actionable recommendations, limitations of our study, and potential areas for future research. The focus of this qualitative study was to gain an in-depth understanding of supply chain risk factors specific to services and to help validate MITRE's SoT framework. As aforementioned, MITRE's SoT serves as a framework for organizations to measure trustworthiness and identify risk factors affecting their supply chain security. We utilized MITRE's taxonomy of supply chain risk factors and explored the services supply chain risks experienced by various DOD organizations through thematic analysis of exploratory interviews. The conclusion follows each of the original questions.

- What are the primary indicators of supply chain risk, and which are unique to DOD services?

We identified six primary indicators of supply chain risk (service performance metrics, customer feedback, cost metrics, external indicators, personnel issues, and procurement fraud), Figure 11: Risk Indicators provides a visualization for each of those indicators and categorizes Service Performance Metrics as the most cited risk indicator unique to DOD services. Furthermore, Table 9: ICOPARS Risk Indicators demonstrates the application of our risk indicator framework. DOD supply chain managers should incorporate these indicators in their acquisition planning to monitor the services aspect of their supply chains. Also, supply chain managers outside the DOD can take these indicators and apply them to their organizations. These indicators are not unique to the DOD.

- What are the best practices for preventing, mitigating, and responding to DOD service specific supply chain risks?

From the data derived from our interviews, we identified four themes of best practices as a mitigation technique to services supply chain risks. As pictured in the Mitigation Technique Model (Figure 12), contract administration is the most prominent method for mitigating supply chain risk. Clearing defining requirements and maintaining unequivocal communication amongst all parties (contractor, customer, and government official) are also prevailing techniques for preventing service specific supply chain risks. Although these best practices do not offer any emerging techniques to managing the service aspect of supply chains, our results demonstrate the importance of planning and communicating to supply chain risk management. Firms like Resilinc offer supply chain mapping services to give organizations insight into their supply chain. According to Resilinc, understanding your own supply chain is a crucial step to managing risk because it allows managers to clearly communicate with each other (Guinto, 2022). The DOD instructs managers to take this step through acquisition planning (FAR 7.105, 2022). Outside the DOD, managers should align their planning and mitigation techniques by adapting these best practices to their own organizational requirements.

B. RECOMMENDATIONS TO MITRE

Our research supports the SoT by closely examining the services aspect of supply chains and drafting frameworks MITRE should consider while completing the SoT taxonomy. In addition to developing our frameworks, we arrived at two direct recommendations to MITRE to improve the services category of the SoT. We ensure our recommendations align with the stated objectives of the SoT framework.

1. Recommendation 1: Adjust Services' Risk Areas

The risk factor themes we identified for each SoT risk area showed an overlap between risk areas. Largely this is due to how the SoT defines security, quality, reliability, and integrity. Upon reviewing our risk factors, shown in Table 5, we found the risk factors tend to gravitate towards three different areas: external, service provider specific, and customer specific. The external risk area refers to risk factors that are external to the relationship built between a service provider and customer. These included the availability of the service in the market, bureaucratic risk factors affecting the ability to perform the

service, and economic risk factors outside the control of either the buyer or seller. The other two risk areas naturally gravitate towards either the service provider or the customer. As demonstrated in the literature, services distinguish themselves due to the involvement of the customer in creation/production. Our results support this idea because several risk factors lie with the customer. These risk factors include contract administration, contract structure, customer risk factors, and requirements generation risk factors. We found the remaining risk factors lie with the service provider. These include counterintelligence risk factors, contractor experience risk factors, personnel risk factors, and supporting infrastructure risk factors. Table 10 shows the hierarchy of the risk factors we identified falling under each unique risk area. We recommend the SoT modify its identified risk areas to incorporate these three areas when considering the services aspect of the supply chain.

Table 10. Recommended SoT Risk Areas and Risk Factors

External Risk Areas	Service Provider Specific Risk Areas	Customer Specific Risk Areas
• Availability Risk Factors • Bureaucratic Risk Factors • Economic Risk Factors	• Counterintelligence Risk Factors • Contractor Experience Risk Factors • Personnel Risk Factors • Supporting Infrastructure Risk Factors	• Contract Administration Risk Factors • Contract Structure Risk Factors • Customer Risk Factors • Requirement Generation Risk Factors

2. Recommendation 2: Performance Monitoring Data Considerations

We recommend the Risk Model Manager (the user interface of the SoT) allow users to account for their organizations' internal performance monitoring when evaluating a supply chain. This recommendation aligns with two of the stated goals of the SoT. The SoT seeks to identify ways to gather evidence relating to the barriers of trust between organizations and allow the SoT to be tailored to specific concerns faced by organizations (Martin et al., 2021). Performance monitoring data provides ongoing evidence of the performance of a service. Within the DOD, managers use this data to continually assess

the relationship with vendors. Adding this consideration also enhances how customizable the tool is for users. Some organizations may not track data for the services aspect of supply chain and may not need to. However, as seen in the ICOPARS use case, tracking customer feedback and website uptime versus downtime provides the managers invaluable data points to assess the services aspect of the supply chain.

Services cannot be measured at a single point in time like a good or a supplier. The heterogeneity aspect of services requires their performance to be measured throughout the performance of the service. Also, the service quality providers expect to deliver may vary from the quality level expected by the customer (Finkenstadt & Hawkins, 2016). Therefore, a reliable performance assessment is difficult to obtain due to these inconsistencies. Also, services require input from the customer. We did not identify nascent data sources for the SoT to pull from to quantifiably measure supply chain risk. Our results do, however, show that program managers evaluate services throughout their performance. The strong number of responses we received regarding contract administration as a mitigation technique supports this argument. Also, many managers we interviewed developed a tool or database intra-organizationally to track performance and customer feedback.

C. SERVICES SUPPLY CHAIN RISK MANAGEMENT FRAMEWORK

After analyzing the results of our interview data, we linked each relevant code from our identified risk factors to corresponding risk indicator codes and risk mitigation codes. To do this, we considered what the indicators for risk would be for each risk factor. We then considered how each risk could be mitigated using the mitigation techniques we identified. This produced a Services Supply Chain Risk Management Framework which offers a 360-degree view of supply chain risk. The results of this analysis can be found in Appendix C. In instances in which we did not identify any mitigation techniques for an associated risk, our framework suggests considering alternative suppliers or substitute service solutions. In Figure 15, we kept the label “none identified” to limit ourselves to the responses from our interviews.

1. Linking Risk Factors to Risk Indicators

The risk indicators reveal a pattern across the different risk areas we recommended to MITRE's SoT. Specifically, COR reports and QASP metrics were the main indicators of risk related to the customer specific risk factors. Figure 14 shows the frequency of each indicator across our three risk areas. COR reports can expose problems from customer education and customer satisfaction. Also, COR reports reveal issues related to the relationship between the service provider and the customer. QASP metrics and performance monitoring may reveal issues with opaque requirements or the alignment between the supply chain and contracting chain. For example, lagging service performance metrics may indicate the vendor does not understand the requirement or the requirement is too poorly defined to have reliable service performance metrics.

There was a significant gap in the risk indicators we identified from our data relating to the external risk areas. This is likely because these risks fall outside the control of supply chain managers. Economic issues, such as a recession, may suggest inflation or high unemployment will be a concern for managers. However, bureaucratic risk factors such as international laws and external approvals lacked a corresponding risk indicator.

Finally, the indicators for the service provider risk areas varied the most. QASP metrics or service performance metrics enables managers to monitor the performance of the service, as shown in the ICOPARS case. These metrics may indicate cyber problems or issues with the supporting infrastructure for a service. The un-availability of a specific service in a business environment may expose a lack of qualified personnel. Another indicator under service provider specific risk areas was past performance. Managers use past performance to evaluate risks related to the capacity of the company to ensure the provider will be able to meet the requirements of the contract.

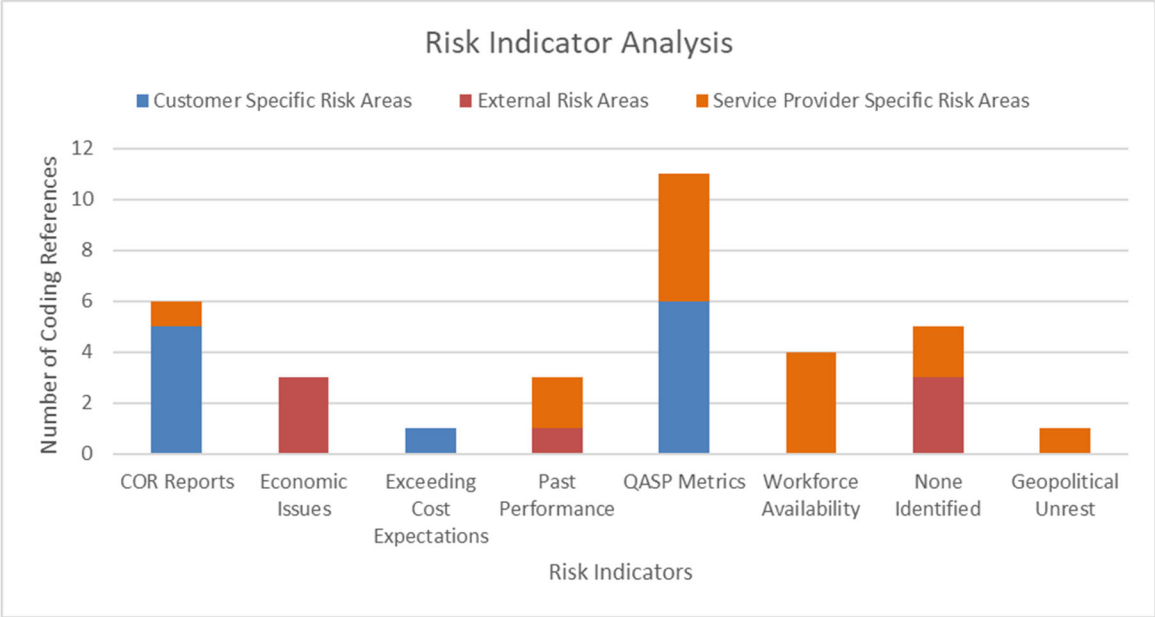


Figure 14. Risk Indicator Analysis

2. Linking Risk Factors to Mitigation Techniques

Figure 15 demonstrates the risk mitigation techniques corresponding with each risk area. The most prominent mitigation technique related to our customer specific risk area was communication between the contractor and customer. Customer/ KTR communication mitigates risks related to customer satisfaction, relationships with the service provider, and alignments within the supply chain and contracting chain. For example, supply chain managers should communicate with contractors throughout the performance of the service in order to adapt to any arising issues. One issue within the federal contracting is privity. The government lacks privity with subcontractors. This creates a barrier preventing the government from actively manage subcontractors as directly as they can with prime contractors. Aligning the contracting chain with the supply chain alleviates the burden of managing organizations vertically because acquisition managers can prioritize relationships. Requirement generation is a mitigation tool used to moderate risks related to opaque requirements or too narrowly defined requirements. Other risk mitigation techniques include security requirements for limiting the use of extraneous security clearance constraints which may unnecessarily limit the pool of available providers. Customer education manages the customer's expectations supporting the perceived service

quality. Finally, COR training or proper training of oversight officials ensures a reliable assessment of the provider's performance.

We linked only one mitigation technique to a risk factor under the external risk areas. Incorporating industry days as part of market research shows managers what services are available to meet their requirement. We did not identify any mitigation techniques related to economic risk factors such as inflation or high unemployment, or bureaucratic risk factors such as international sanctions or shipping restrictions. As previously discussed with the risk indicators, these risks are external to the relationship between the supplier and vendor. Depending on the situation, managers may adapt through a robust and agile supply chain. In these situations, the mitigation technique will be dictated by the environment and will depend on the specific circumstances.

The mitigation techniques for risks carried by service providers largely involved service performance metrics and requirement generation. Service performance metrics control supporting infrastructure risks and cyber risks. For example, if logistic issues begin delaying the shipment parts, managers monitoring lead times will be able to respond with more agility and adapt to a dynamic risk environment. Also, monitoring website metrics helps managers uncover the presence of cyber issues. Requirement generation refers to ensuring managers establish clear and well-written requirements. This mitigation technique corresponds to ensuring the vendor maintains qualified personnel to perform a service. We also identify security requirements, contract structure, and communication between the vendor and customer as relating to the service provider risk areas. Security requirements protect against information leakage. The contract structure may prevent risks relating to the origin of supplies. Finally, communication with the vendor mitigates risk related to relying on the vendor to address security issues.

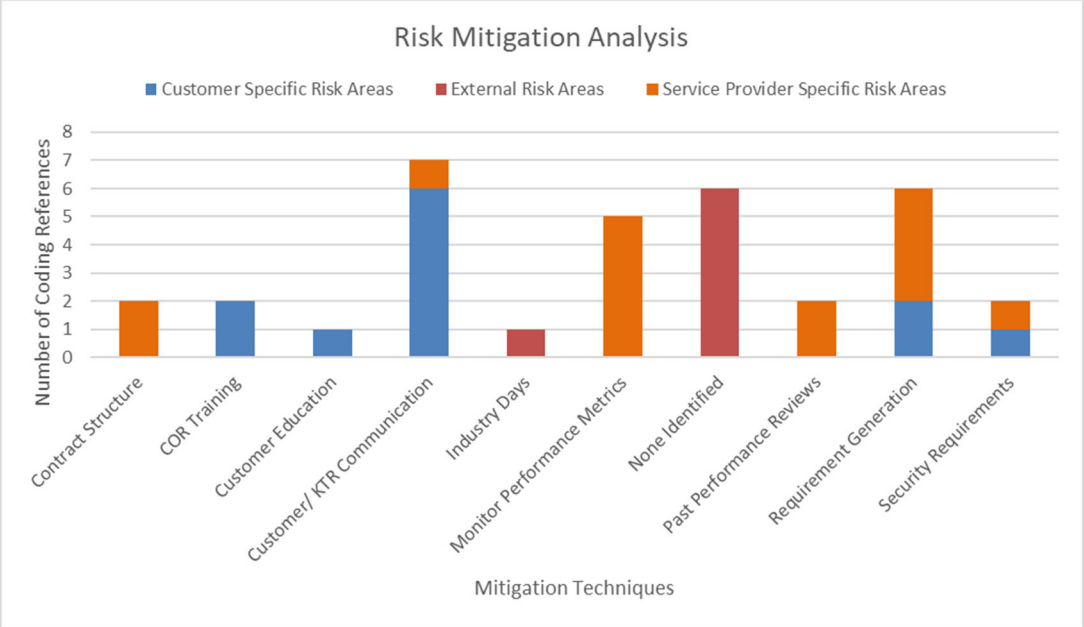


Figure 15. Risk Mitigation Analysis

3. Recommendation to DOD Acquisition Managers

We recommend DOD acquisition managers apply our framework to contract acquisition plans. Even though our framework looks at services risk factors, it is applicable to contracts for both services and supplies. As shown with ICOPARS, supply contracts may entail service components that carry unique risks which managers need to consider. In fact new research in marketing around service dominant logic contends that services, not goods, is fundamental to economic exchange (Vargo & Lusch, 2004). Our Services Supply Chain Risk Management Framework provides these managers a tool to consider different service-specific risks that could affect the acquisition. To use our framework, managers start with the services risk factors and consider how they apply to their situation. By linking risk factors to risk indicators, we show indicators of these risks that managers can incorporate in their QASP. Finally, by linking mitigation techniques to risk factors, we show the best practices to manage or mitigate these risks.

D. LIMITATIONS OF OUR STUDY AND CONSIDERATIONS FOR FUTURE RESEARCH

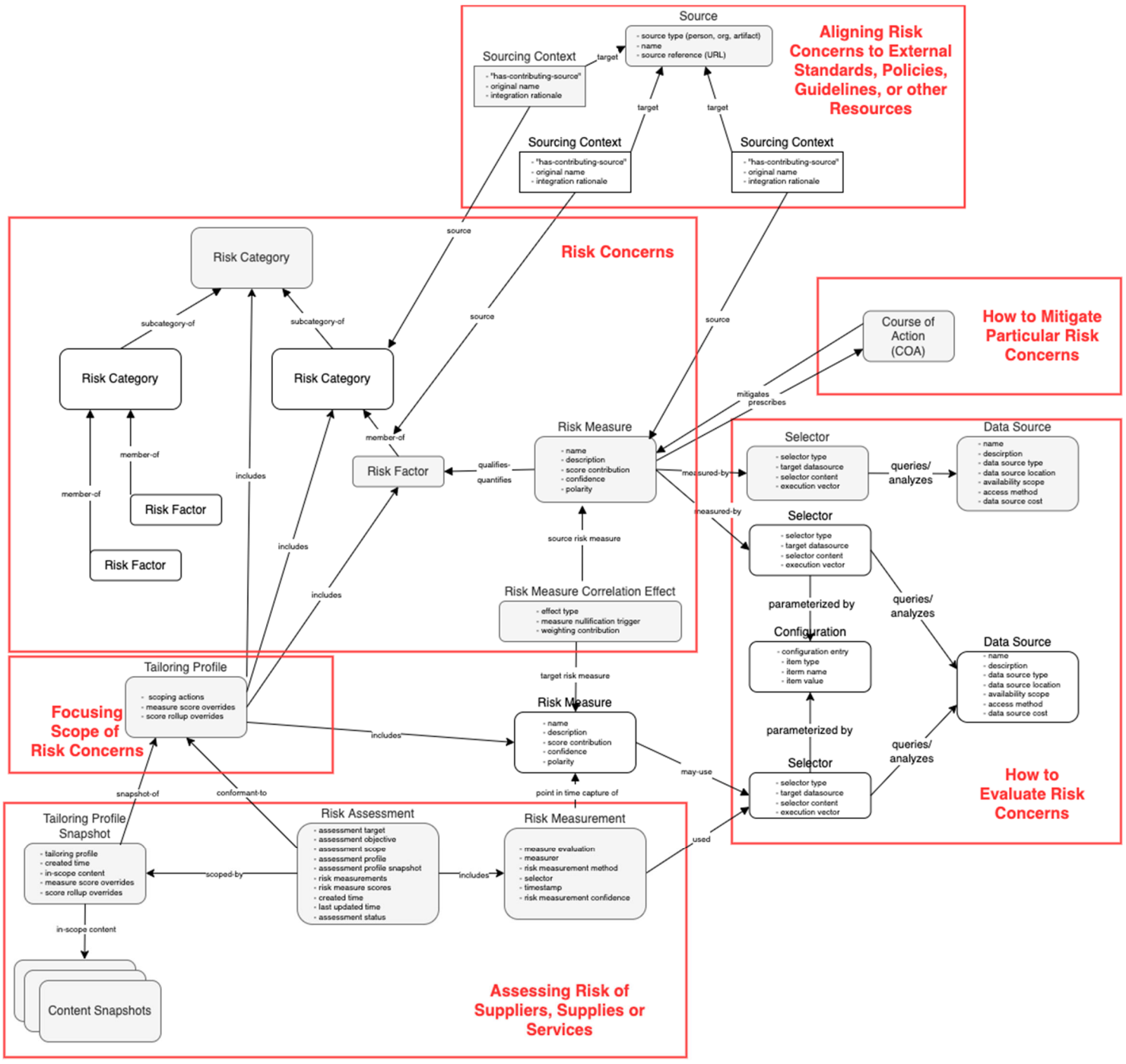
Services vary greatly in nature. The supply chain risks associated with painting a house diverge from the supply chain risks involved in maintaining a website. Managers using our framework to consider services related supply chain risks need to apply discretion to determine if a risk factor applies to their environment. Our Services Supply Chain Risk Management Framework offers areas of general concern when evaluating a services supply chain but does not capture every potential risk to services supply chains. Also, our interviewees included only DOD acquisition professionals. Furthermore, six of the nine interviews we conducted consisted of strictly Air Force acquisition professionals. This presents a concern with external validity bias. Future research should replicate our study with a more diverse interviewee pool to validate the risk factors we identified external to the Air Force and to government contracting.

Finally, we present the results of our analysis with values showing the number of coding references of each theme we found in our interview data. These values do not suggest one theme is more important than another. We provide these values to portray data saturation within our interview data. Our framework also does not offer a hierarchy of risk and should not be interpreted as a predictive model of supply chain risk. Future research into services specific supply chain risk should conduct a more robust analysis to quantify the impacts of risk factors on a supply chain. This would go beyond our research and be useful in quantifying the amount of supply chain risk impact given a situation like a conditional probability model.

Our research primarily sought to inform MITRE's SoT framework by validating their services risk taxonomy. Throughout our process, we not only found a clearer way of evaluating services supply chain risk, but we also developed a framework managers should use to better manage risk and create agile, adaptable, and aligned supply chains. Managers will not always be able to foresee and manage every potential supply chain disruption. However, others should build off our research to continue identifying supply chain risks and mitigation techniques to create more resilient and agile supply chains.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SYSTEM OF TRUST STRUCTURE



THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. IN-PROGRESS SYSTEM OF TRUST TOP-LEVEL RISK CATEGORIES

Supply Chain Security Risks

Supplier Risks							Supply Risks			Service Risks			
External Influences	Financial Stability	Organizational Stature	Susceptibility	Quality Culture	Maliciousness	Organizational Security	Hygiene	Malicious Taint	Counterfeit	Integrity of Service Delivered	Quality of Service Delivered	Reliability of Service Delivered	Security of Service Delivered
Foreign relationships	Questionable debt management	Corporate ownership reputation	Customers	Company has a low CMMI rating	Foreign Intelligence Service (FIS) influence	Concerns regarding facility access	Product quality	Facilities integrity	Copycat manufacturing	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree
Operational location concerns	Questionable financial stewardship	Diversity and inclusion	Industry sector	Internal company QC, SCRM policy & practice	Fraud and corruption	Concerns regarding software access	Product resilience	Functional integrity	Mislabeling	Service Infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance
Foreign registration/ incorporation	Questionable future outlook	Geographic concentration	Location	Subcontractor supply chain health / risk	Legal/law issues	Concerns regarding hardware access	Product security	Geopolitical integrity	Packaging integrity	Service specific integrity	Service specific quality	Service specific reliability	Service specific security
Geopolitical instability	Questionable profitability	Mergers & acquisitions frequency	Personnel		Sanction list status	Cyber threat activity		Logistics / transportation integrity	Technical authenticity				
Key Management Personnel (KMP) and non-person entity relationships	Vulnerability of financial stability to foreign influence	Natural disasters	Technical susceptibility			Data security status		Maintenance integrity	Unsanctioned manufacturing				
National corruption	Vulnerability of financial stability to market factors	Operational volatility				Type/ level /frequency of security training		Manufacturing process integrity					
National governance	Vulnerability to takeover	Sustainability				Vulnerabilities		Packaging integrity					
Organization ownership and control								Reputational integrity					
Politically Exposed Persons (PEPs) in corporate leadership								Supply chain integrity					
Political vulnerability													
Transparency of organization control													

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. SERVICES SUPPLY CHAIN RISK MANAGEMENT FRAMEWORK

SoT Risk Area	Recommended Risk Area	Risk Factor Theme	Relevant Code	Risk Indicator	Risk Mitigation Technique
Security Risk Area	Customer Specific Risk Areas	Contract Structure Risk Factors	Supply Chain and Contracting Chain Alignment	QASP Metrics	Customer/ KTR Communication
Security Risk Area	Customer Specific Risk Areas	Contract Structure Risk Factors	Excessive Security Requirements	Exceeding Cost Expectations	Security Requirements
Reliability Risk Area	Customer Specific Risk Areas	Contract Structure Risk Factors	Supply Chain and Contracting Chain Alignment	QASP Metrics	Customer/ KTR Communication
Quality Risk Area	Customer Specific Risk Areas	Customer Risk Factors	Customer Education	COR Reports	Customer Education
Quality Risk Area	Customer Specific Risk Areas	Customer Risk Factors	Customer Relationship with Service Provider	COR Reports	Customer/ KTR Communication
Quality Risk Area	Customer Specific Risk Areas	Contract Administration Risk Factors	COR Training	QASP Metrics	COR Training
Quality Risk Area	Customer Specific Risk Areas	Requirement Generation Risk Factors	Opaque Requirements	QASP Metrics	Requirement Generation
Quality Risk Area	Customer Specific Risk Areas	Customer Risk Factors	Customer Satisfaction	COR Reports	Customer/ KTR Communication
Integrity Risk Area	Customer Specific Risk Areas	Requirement Generation Risk Factors	Opaque Requirements	QASP Metrics	Requirement Generation
Integrity Risk Area	Customer Specific Risk Areas	Customer Risk Factors	Customer Relationship with Service Provider	COR Reports	Customer/ KTR Communication
Integrity Risk Area	Customer Specific Risk Areas	Customer Risk Factors	Customer Satisfaction	COR Reports	Customer/ KTR Communication
Integrity Risk Area	Customer Specific Risk Areas	Contract Administration Risk Factors	Qualified oversight officials	QASP Metrics	COR Training
Security Risk Area	External Risk Areas	Bureaucratic Risk Factors	International Laws	None Identified	Alternative Suppliers or Substitute

SoT Risk Area	Recommended Risk Area	Risk Factor Theme	Relevant Code	Risk Indicator	Risk Mitigation Technique
					Service Solutions
Reliability Risk Area	External Risk Areas	Availability Risk Factors	Service Availability	Past Performance	Industry Days
Reliability Risk Area	External Risk Areas	Bureaucratic Risk Factors	International Shipping Restrictions	None Identified	Suppliers or Substitute Service Solutions
Reliability Risk Area	External Risk Areas	Economic Risk Factors	Inflation	Economic Issues	Suppliers or Substitute Service Solutions
Quality Risk Area	External Risk Areas	Bureaucratic Risk Factors	External approvals to perform service	None Identified	Suppliers or Substitute Service Solutions
Integrity Risk Area	External Risk Areas	Economic Risk Factors	Inflation	Economic Issues	Suppliers or Substitute Service Solutions
Integrity Risk Area	External Risk Areas	Economic Risk Factors	Unemployment	Economic Issues	Suppliers or Substitute Service Solutions
Security Risk Area	Service Provider Specific Risk Areas	CI Risk Factors	Information Leakage	None Identified	Security Requirements
Security Risk Area	Service Provider Specific Risk Areas	Personnel Risk Factors	Number of Parties Involved	None Identified	Contract Structure
Security Risk Area	Service Provider Specific Risk Areas	Personnel Risk Factors	Reliance on KTRs to Address Security Issues	COR Reports	Customer/ KTR Communication
Security Risk Area	Service Provider Specific Risk Areas	CI Risk Factors	Origin of Supplies	Geopolitical Unrest	Contract Structure
Security Risk Area	Service Provider Specific Risk Areas	CI Risk Factors	Cyber	QASP Metrics	Monitor Service Performance Metrics

SoT Risk Area	Recommended Risk Area	Risk Factor Theme	Relevant Code	Risk Indicator	Risk Mitigation Technique
Reliability Risk Area	Service Provider Specific Risk Areas	Supporting Infrastructure Risk Factors	Company Capacity	Past Performance	Past Performance Reviews
Reliability Risk Area	Service Provider Specific Risk Areas	Personnel Risk Factors	Qualified Personnel	Workforce Availability	Requirement Generation
Reliability Risk Area	Service Provider Specific Risk Areas	Supporting Infrastructure Risk Factors	Service Enabling Supplies	QASP Metrics	Monitor Service Performance Metrics
Quality Risk Area	Service Provider Specific Risk Areas	Personnel Risk Factors	Qualified Personnel	Workforce Availability	Requirement Generation
Quality Risk Area	Service Provider Specific Risk Areas	Contractor Experience Risk Factors	Evaluating relevant past performance	Past Performance	Past Performance Reviews
Quality Risk Area	Service Provider Specific Risk Areas	Supporting Infrastructure Risk Factors	Service Enabling Supplies	QASP Metrics	Monitor Service Performance Metrics
Quality Risk Area	Service Provider Specific Risk Areas	Personnel Risk Factors	Personnel Turnover	Workforce Availability	Requirement Generation
Integrity Risk Area	Service Provider Specific Risk Areas	Supporting Infrastructure Risk Factors	Availability of supporting systems	QASP Metrics	Monitor Service Performance Metrics
Integrity Risk Area	Service Provider Specific Risk Areas	Supporting Infrastructure Risk Factors	Reliance on third parties to support service	QASP Metrics	Monitor Service Performance Metrics
Integrity Risk Area	Service Provider Specific Risk Areas	Personnel Risk Factors	Qualified Personnel	Workforce Availability	Requirement Generation

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. RISK FACTOR DEFINITIONS

Risk Factor Name	Definition
Availability Risk Factors	Constraints caused by the availability of the service in the marketplace
Bureaucratic Risk Factors	Constraints caused by legal or regulatory barriers impeding the performance of a service
CI Risk Factors	Constraints caused by adversarial malicious efforts
Contract Administration Risk Factors	Constraints related to the oversight of a service's performance
Contract Structure Risk Factors	Constraints caused by the structure or nature of the agreement connecting all parties involved in a service
Contractor Experience Risk Factors	Constraints caused by the experience or performance history of the service provider
Customer Risk Factors	Constraints related to the customer's relationship with the service provider to include customer education and perceived service quality
Economic Risk Factors	Constraints related to external economic conditions
Personnel Risk Factors	Constraints related to the reliability of the personnel performing the service
Requirement Generation Risk Factors	Constraints caused by miscommunicating or providing poorly written requirements
Supporting Infrastructure Risk Factors	Constraints related to the reliability of the systems and supplies necessary to perform the service

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, W.C. (2015) Conducting Semi-Structured Interviews. In Wholey, J.S., Harty, H.P. and Newcomer, K.E. (Eds.), *Handbook of Practical Program Evaluation* (pp. 492–505). Jossey-Bass. https://doi.org/10.1002/9781119171386.ch19

AIMS. (2022, February 16). *SCOR Model*. Academy for International Modern Studies. https://aims.education/study-online/supply-chain-operations-reference-model-scor/

Apte, A., Apte, U., & Rendon, R. (2010). Services supply chain in the Department of Defense: Comparison and analysis of acquisition management in the Army, Navy, and Air Force. Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/33484.

Apte, U., Ferrer G., Lewis I., & Rendon R. (2006). Managing the service supply chain in the Department of Defense: Opportunities and challenges. *Third Annual Acquisition Research Symposium*, 372–402. https://www.researchgate.net/publication/242230814_MANAGING_THE_SERVICES_SUPPLY_CHAIN_IN_THE_DEPARTMENT_OF_DEFENSE_OPPORTUNITIES_AND_CHALLENGES

Aqlan, F., & Lam, S. (2015). A fuzzy-based integrated framework for supply chain risk assessment. *International Journal of Production Economics, 161*, 54–63. https://doi.org/10.1016/j.ijpe.2014.11.013

Assad, S. (2012, August 27). Taxonomy for the Acquisition of Services and Supplies & Equipment [Memorandum]. Department of Defense.

Boer, L., Labro, E., & Morlacchi, P. (2001). A review of methods supporting supplier selection. *European Journal of Purchasing & Supply Management*, *7*(2), 75–89. https://doi.org/10.1016/s0969-7012(00)00028-9

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2019). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health, 13*(2), 201–216. https://doi.org/10.1080/2159676X.2019.1704846

Center for Strategic and International Studies (CSIS). (2022, 5 July). *Significant Cyber Incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chopra, S., & Meindl, P. (2013). *Supply chain management: strategy, planning and operation* (5th ed.). Prentice Hall.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46*(1), 53–61. https://libproxy.nps.edu/login?url=https://www-proquest-com.libproxy.nps.edu/scholarly-journals/managing-risk-avoid-supply-chain-breakdown/docview/224964486/se-2?accountid=12702

Christopher, M., & Holweg, M. (2011). "Supply Chain 2.0": Managing supply chains in the era of turbulence. *International Journal of Physical Distribution & Logistics Management*, *41*(1), 63–82. https://doi.org/10.1108/09600031111101439

Christopher, M., & Peck, H. (2004). Building the Resilient Supply Chain. *The International Journal of Logistics Management*, *15*(2), 1–14. https://doi.org/10.1108/09574090410700275

Cooper, M. & Ellram, L. M. (1993). Characteristics of supply chain management and the implications for purchasing and logistics strategy. *The International Journal of Logistics Management, 4*(2), 13–24. https://doi.org/10.1108/09574099310804957

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry & research design: Choosing among five approaches. SAGE Publication Inc.

Defense Acquisition University. (2003). *Risk management guide for DOD acquisition* (5th ed.). Department of Defense. https://apps.dtic.mil/sti/pdfs/ADA437820.pdf

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health, 7*(2). https://doi.org/10.1136/fmch-2018-000057

Department of Defense. (2019, March 6). *DOD supply chain materiel management policy* (DOD Instruction 4140.01). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/414001p.pdf

Department of Defense. (2022). *Securing defense-critical supply chains: An action plan developed in response to President Biden's executive order 14017.* https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

Department of Labor. (2022a). *Major occupational groups as a percentage of total employment* [Data table]. U.S. Bureau of Labor Statistics. https://www.bls.gov/oes/2021/may/featured_data.htm#largest3

Department of Labor. (2022b). *Industries at a glance* [Data table]. U.S. Bureau of Labor Statistics. https://www.bls.gov/iag/tgs/iag07.htm

DiNapoli, T. J., (2021). Service acquisitions: DOD's report to Congress identifies steps taken to improve management, but does not address some key planning issues. (GAO-21-267R). Government Accountability Office.

Ellram, L. M., Tate, W. L., & Billington, C. (2007). Services supply management: The next frontier for improved organizational performance. *California Management Review, 49*(4), 44–66. https://doi.org/10.2307/41166405

Exec. Order No. 14017, 3 C.F.R. (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

FAR 7.105, Contents of Written Acquisition Plans (2022). https://www.acquisition.gov/far/7.105

FAR 37.101, Definitions (2022). https://www.acquisition.gov/far/37.101

FAR 37.102, Policy (2022). https://www.acquisition.gov/far/37.102

FAR 37.602, Performance Work Statement (2022). https://www.acquisition.gov/far/37.602

Feizabadi, J., Maloni, M., & Gligor, D. (2019). Benchmarking the triple-A supply chain: orchestrating agility, adaptability, and alignment. *Benchmarking: an International Journal*, *26*(1), 271–295. https://doi.org/10.1108/BIJ-03-2018-0059

Finkenstadt, D. J. (2020). *Essays on perceived service quality and perceived value in business-to-government knowledge-based services* [Doctoral dissertation, University of North Carolina at Chapel Hill]. UNC Chapel Hill Library. https://doi.org/10.17615/50cn-4579

Finkenstadt, D. J., & Hawkins, T. G. (2016). #eVALUate: Monetizing service acquisition trade-offs using the Quality-Infused Price© methodology. *Defense Acquisition Research Journal, 23*(2), pp. 202–230.

Gaudenzi, B., & Borghesi, A. (2006). Managing risks in the supply chain using the AHP method. *International Journal of Logistics Management*, *17*(1), 114–136. https://doi.org/10.1108/09574090610663464

Gronroos, C. (1988). Service quality: The six criteria of good perceived service quality. *Review of Business, 9*(3), pp. 10–13. https://www.proquest.com/docview/220949893/fulltextPDF/49F61EF8312943CDPQ/1?accountid=12702

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PloS One, 15*(5). https://doi.org/10.1371/journal.pone.0232076

Guinto, P. (2022, September 8). *Overview of recent supply chain issues* [Presentation]. Supply Chain and Sourcing Education and Training for National Defense], Naval Postgraduate School, Dudley Knox Library.

Handfield, R., Apte, A., & Finkenstadt, D. J. (2022). Developing supply chain immunity for future pandemic disruptions. *Journal of Humanitarian Logistics and Supply Chain Management*. https://doi.org/10.1108/JHLSCM-09-2021-0096

Handfield, R., Finkenstadt, D. J., & Guinto P. (2021, February 15). How business leaders can prepare for the next health crisis. *Harvard Business Review.* https://hbr.org/2021/02/how-business-leaders-can-prepare-for-the-next-health-crisis

Handfield, R., Finkenstadt, D. J., Schneller, E. S., Godfrey, A.B., & Guinto, P. (2020). A commons for a supply chain in the post-COVID-19 era: The case for a reformed strategic national stockpile. *The Milbank Quarterly, 98*(4) 1058–1090. https://doi.org/10.1111/1468-0009.12485

Handfield, R. & Linton, T. (2022). *Flow: How the best supply chains thrive.* University of Toronto Press.

Harrell, M. & Bradley, M. (2009). *Data Collection Methods: Semi-Structured Interviews and Focus Groups*. RAND. https://www.rand.org/pubs/technical_reports/TR718.html

Harris, C. (2020). *Information technology: Federal agencies need to take urgent action to manage supply chain risks* (GAO-21-171). Government Accountability Office. https://www.gao.gov/products/gao-21-171

Hawkins, T.G., Gravier, M.J., Berkowitz, D. & Muir, W.A. (2015). Improving services supply management in the defense sector: How the procurement process affects B2B service quality. *Journal of Purchasing and Supply Management, 21*(2), pp.81-94. https://www.researchgate.net/publication/271225861_Improving_services_supply_management_in_the_defense_sector_How_the_procurement_process_affects_B2B_service_quality

Haywood-Farmer, J. (1988). A conceptual model of service quality. *International Journal of Operations & Production Management, 8*(6) 19–29. https://doi.org/10.1108/eb054839

Juttner, U., Peck, H., & Martin, C., (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics 6*(4), pp. 197–210. https://doi.org/10.1080/1367556031000162701 6

Kamal M., & Irani, Z. (2014). Analysing supply chain integration through a systematic literature review: A normative perspective. *Supply Chain Management*, *19*(5/6), 523–557. https://doi.org/10.1108/SCM-12-2013-0491

La Londe, B. J., & Masters, J. M. (1994). Emerging logistics strategies: Blueprints for the next century. *International Journal of Physical Distribution & Logistics Management, 24*(7), 35–47. https://doi.org/10.1108/09600039410070975

Lee, H. L. (2004), The triple-A supply chain, *Harvard Business Review, 82*(10), 102–112. https://hbr.org/2004/10/the-triple-a-supply-chain

Li, L., Su, Q., & Chen, X. (2011). Ensuring supply chain quality performance through applying the SCOR model. *International Journal of Production Research, 49*(1), 33–57. https://doi.org/10.1080/00207543.2010.508934

Martin, R. A. (2020a). *Trusting our supply chains: A comprehensive data-driven approach* (Report No. 20–01465-37). MITRE. https://www.mitre.org/sites/default/files/publications/pr-20-01465-37-trusting-our-supply-chains-a-comprehensive-data-driven-approach.pdf

Martin, R. A. (2020b). The supply chain security system of trust: A framework for the concerns blocking trust in supplies, suppliers, and services. *Cutter Businesss Technology Journal, 33*(5). https://www.cutter.com/article/supply-chain-security-system-trust-framework-concerns-blocking-trust-supplies-suppliers-and

Martin, R. A., Barsoum, Y., Hall, J. B. & Aisenberg, M. A. (2021). Defining a system of trust as a keystone tool for supply chain security. *The SciTech Lawyer, 17*(2), 20–28.

Parasuraman, A., Zeithaml, V., and Berry, L. (1985). A conceptual model of service quality and its implications for future research. *Journal of Marketing, 49*(4), pp. 41–50. https://doi.org/10.2307/1251430

Peters, H. M. (2021). Defense primer: Department of Defense contractors (CRS Report No. IF10600). Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF10600

Pettit, T., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics*, *31*(1), 1–21. https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

Pettit, T. T., Croxton, K. L., & Fiskel, J., T. T. (2019). The evolution of resilience in supply chain management: A retrospective on ensuring supply chain resilience. *Journal of Business Logistics, 40*(1), 56–65. https://doi.org/10.1111/jbl.12202

Pujawan, I. N., & Geraldin, L. H. (2009). House of risk: A model for proactive supply chain risk management. *Business Process Management Journal, 15*(6), 953–967. http://dx.doi.org/10.1108/14637150911003801

Reeder, J., & Hall, T. (2021). Cybersecurity's Pearl Harbor moment: Lessons learned from the Colonial Pipeline ransomware attack. *The Cyber Defense Review, 6*(3), 15–40.

Ripley, M. (2021). *MITRE System of Trust* (Case No. 21–01357-20). MITRE.

Rizkya, I. Syahputri, K., Sari, R., Siregar, I., & Utaminingrum, J. (2019). SCOR: Business process analysis and supply chain performance in building materials industry. *IOP Conference Series. Materials Science and Engineering*, *598*(1). https://doi.org/10.1088/1757-899X/598/1/012070

Selviaridis, K., & Norrman, A. (2014). Performance-based contracting in service supply chains: A service provider risk perspective. *Supply Chain Management, 19*(2), 153–172. http://dx.doi.org/10.1108/SCM-06-2013-0216.

Schiffling, S., & Kanellos, N. K. (2022, September 7). 5 challenges facing global supply chains. *World Economic Forum.* https://www.weforum.org/agenda/2022/09/5-challenges-global-supply-chains-trade/

Shashi, K., Centobelli, P., Cerchione, R., & Ertz, M. (2020). Managing supply chain resilience to pursue business and environmental strategies. *Business Strategy and the Environment*, *29*(3), 1215–1246. https://doi.org/10.1002/bse.2428

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488. https://doi.org/10.1016/j.ijpe.2005.12.006

Tong, X., Lai, K., Lo, C., & Cheng, T. (2022). Supply chain security certification and operational performance: The role of upstream complexity. *International Journal of Production Economics*, 247. https://doi.org/10.1016/j.ijpe.2022.108433

Vargo, S. L., & Lusch, R. F. (2004). Evolving to a New Dominant Logic for Marketing. *Journal of Marketing*, *68*(1), 1–17. https://doi.org/10.1509/jmkg.68.1.1.24036

Veselovska, L. (2020). Supply chain disruptions in the context of early stages of the global COVID-19 outbreak. *Problems and Perspectives in Management, 18*(2), 490–500. https://doi.org/10.21511/ppm.18(2).2020.40

Whitaker, B. (2021). SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments. *CBS News.* https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-07-04/

White House. (2021). Building resilient supply chains, revitalizing American manufacturing, and fostering broad-based growth. https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School