THE CISO ROLE WITHIN U.S. FEDERAL GOVERNMENT CONTRACTING ORGANIZATIONS: A DELPHI STUDY

By

Darren Death

SHARDUL PANDYA, PhD, Faculty Mentor and Chair

OLUDOTUN ONI, PhD, Committee Member

AHMAD MOSTAFA, PhD, Committee Member

Todd C. Wilson, PhD, Dean School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Information Technology

Capella University

December 2020

© Darren Death, 2020

Abstract

Government suppliers provide critical services to the U.S. federal government. The government presents a large target for groups such as nation-states, attackers, and organized crime. Due to the large attack surface the U.S. federal government offers, government contractors must secure their information technology infrastructures to reduce this threat surface from a third-party risk management perspective. Determining the critical roles for the success of the CISO within a U.S. federal government contracting organization is crucial to ensuring the security and resiliency of the government supplier and their federal customer. The purpose of this qualitative classical Delphi study is to identify the roles of the chief information security officer (CISO) in a government contracting organization as viewed by a panel of cybersecurity experts and to determine the extent to which there is a consensus among these experts related to the identified roles. A qualitative methodology was selected for this study as limited information is available related to the chief information security officer's role. The study utilized questionnaires and expert interviews to gather data and develop an understanding of the role of the CISO within a government contracting organization. This study's population consisted of cybersecurity experts who currently hold or have held a position of leadership related to the field of cybersecurity within an organization that supports the U.S. federal government in a contracting capacity. The 19 individuals who participated in the study have immediate responsibility for ensuring that cybersecurity requirements are implemented within their organizations and are responsible for delivering cybersecurity capabilities that allow their organizations to meet the U.S. federal government contracting cybersecurity requirements. The data collected in the Round 1, Round 2, and Round 3 surveys consisted of open-ended questions and a predefined listing of roles. The data analysis involved conducting a thorough examination of the participant's responses. These

responses were synthesized into a single narrative that could be delivered to the expert panel in subsequent rounds to gain consensus related to both the roles critical to the government contracting CISO and the definition of those roles allowing for a consistent understanding of what those roles mean. The study also collected free form responses from the participants. These responses were used to provide further insight as it relates to the various roles of the CISO, the placement of the CISO within the organization, and what needs to be in place for the CISO to be successful related to implementing U.S. federal government cybersecurity requirements. This research directly contributes to the federal government's goals related to contractor security and supply chain management in addition to supplying the government contractor with the information needed to align the CISO role more effectively within their organizations. The information provided by this research in the form of a literature review, roles, role definitions, and CISO reporting structure serves to provide the government supplier with the information needed to ensure that cybersecurity is integrated into the organization. Once integrated, cybersecurity activities can be led by the CISO, who can combine both the technical and business aspects of cybersecurity to manage risk and drive organizational resiliency.

Dedication

This research is dedicated to my wife Mindy Death and my children, who provided me with the love, support, and encouragement necessary to complete my doctoral program. My wife provided me with incredible support throughout the doctoral journey. This support allowed me to focus on the classes I was taking and the research I was conducting. Throughout the entire research process, she additionally supported me by reviewing and editing my work, which served to ensure excellence in my final products. Without the sacrifice of time and resources from my family, I would not have been able to focus my attention on the workload demanded from me. I also dedicate this research to my mother and father, who have always supported me in my educational pursuits and have always been quick to encourage. Without these people's support, conducting this research, and completing my doctoral journey, would have been very difficult.

Thank you.

Acknowledgments

I would like to recognize my mentor and doctoral committee chair, Dr. Shardul Pandya, for his support and counsel throughout my doctoral journey. I would also like to acknowledge my other committee members Dr. Oludotun Oni and Dr. Ahmad Mostafa, who supported me in completing this doctoral program. I would also like to recognize those within my place of employment that helped me in my educational pursuits. Leif Henecke and Dr. Harriet Feldman. Leif was always a supporter of my education, providing me with many of the tools and resources needed to succeed. Harriet provided me with much-needed insight as someone who had already completed her doctoral journey. These individuals provided me with support and encouragement that helped me to accomplish my academic goals.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

The chief information security officer is responsible for maintaining an organization's digital infrastructure's overall security and resiliency. As organizations shift to a more strategic approach to cybersecurity as part of their modernization and innovation strategies, and in response to continuous cyber-attacks and increased U.S. federal government cybersecurity requirements and regulations, the role of the CISO will move to be a role with more prominence (Karanja & Rosso, 2017). The role that the CISO plays in the organization and how the role will mature over time in the U.S. federal government contracting organization is an important area of research (Lanz, 2017). As organizations work to implement new technologies to support business requirements and modernization efforts, the CISO will play a vital role in managing the organization's digital security challenges (Karanja, 2017). Integrating a seasoned CISO into the organization's mission and business capabilities are critical to ensure that a company is compliant from a regulatory perspective. Effective integration of the CISO will also ensure the organization is secure against modern cybersecurity threats, which may harm an organization's capability to meet its business objectives (Pullin, 2018).

This study explores how government contracting leaders might strategically align the CISO role to better plan for and utilize the role to ensure business resiliency and competitiveness. The general problem is that government contracting organizations face the threat of not establishing new or maintain existing contractual work as a result of non-compliance with U.S. federal cybersecurity requirements. This problem, confounded by the ever-growing pace of digital transformation in our nation (Andriole, 2017), brings into focus the need for a clear understanding of the role of the CISO.

The remainder of chapter one covers the following topics: background, business technical problem, research purpose, research questions, rationale, conceptual framework, significance, definition of terms, assumptions and limitations, and the organization of the remainder of the study. The background section presents relevant information about the cybersecurity threat landscape and the intensifying cybersecurity requirements being applied to government contracting organizations. The specific problem that must be mitigated by government contracting organizations related to the chief information security officer is then defined and expanded upon in the next two sections. This leads to the research questions for this study. The rationale and significance sections discuss why this research should be performed and the phenomenon that aligns with the investigation's technical business problem. The significance section describes how this study adds to the overall body of knowledge. Finally, definitions that govern this study are presented, followed by assumptions and limitations that govern this proposed study.

Background

The U.S. federal government is vital to the safety and well-being of the United States and its citizens (Morgeson & Petrescu, 2011). Government contracting organizations provide essential services to the U.S. federal government. Severe disruption to the citizen services could result if these services are not offered securely, as damage could result to the mission of the U.S. federal government agencies (Carter, Weerakkody, Phillips, & Dwivedi, 2016). Agencies are implementing advanced technologies to support their constituencies and meet the mission challenge of higher customer service and increased speed related to service delivery (Gregor & Lee-Archer, 2016). Additionally, agencies have established requirements that ensure their suppliers are meeting cybersecurity requirements that ensure secure development and delivery of

services to the government. The government supplier's security is essential as sensitive government information exists on government contractor networks. Sensitive government information exists on contractor networks due to contractor management processes and direct requests from the government to store and manage sensitive governmental information on supplier networks.

Information technology plays an ever-increasing role in the government contractor's mission performance due to the value that IT brings to mission delivery and contract execution success (Mithas & Rust, 2016). As digital systems have proliferated across government contractor enterprises, the need to protect sensitive governmental information on those systems has become a priority (Doubleday, 2019). The U.S. federal government has developed and has promulgated standards to ensure sensitive governmental information residing on government contractor digital systems are safeguarded (Ross, Dempsey, Viscuso, Riddle, & Guissanie, 2018). Measures such as these are designed to motivate the government contractor community to make more secure choices related to their implementation of information systems that support U.S. federal contracts (Reagin & Gentry, 2018). This approach to incorporating government cybersecurity requirements into the contracting organization must be fully integrated into the mission and strategic planning areas of contracting organizations, helping to ensure that information technology efforts focus on delivering benefits to the organization's mission in a secure manner (Doherty, Ashurst, & Peppard, 2012).

Regulations and standards exist for securing U.S. federal government contractor systems. The National Institutes of Standards and Technology (NIST) and the Department of Defense (DOD) have released cybersecurity standards and guidance that provide the government contractor community with the information necessary to establish cybersecurity controls within

their enterprise networks and information systems (Ross et al., 2018; Sweeney, 2018). The U.S. federal government published guidance for the contracting community that provides the necessary information to formulate plans to establish a cybersecurity program within their respective contractor organizations. The successful execution of these plans supports the government's requirements of protecting sensitive government information that may reside on contractor networks (Dombora, 2016). These regulations and standards serve to provide motivation and guidance for organizations to follow when implementing security controls throughout their organization in accordance with federal requirements (Gikas, 2010).

Ineffective cybersecurity practices are causally linked to information technology intrusions leading to business fraud and exposure. The 2017 FBI Internet Crime Report shows that victim losses related to cybercrime in the U.S. exceeded $1.4 Billion in 2017 (FBI, 2018). In many cases, fundamental cyber hygiene practices were being ignored by an organization's information technology professionals. This lack of attention did not provide the organizations with the necessary operational, technical, and management capabilities to resist an attack. The 2018 Global Megatrends Report published by the Ponemon institute highlighted that cybersecurity is not considered a strategic priority for many organizations within their overall information technology portfolio (Ponemon Institute, 2018). Due to the low strategic importance placed on cybersecurity across many organizations, adequate resources related to people, processes, and technologies are not applied to secure organizational information technology resources. The implementation of information technology capabilities and resources within the enterprise has seen unprecedented growth due to the expected mission value generated via information technology to support mission delivery (Mithas & Rust, 2016). This growth is additionally supported by the CompTIA IT Industry Outlook study, which found that the United

States consumed $1.5 Trillion in information technology solutions in 2018 (CompTIA, 2018). Analyzing the roles of CISOs in U.S. federal government contracting organizations serves to inform better the leadership of contracting organizations (Sabherwal, Sabherwal, Havaknor, Steelman, University of Arkansas, University of Texas-Arlington, & Temple University, 2019). This knowledge will empower leaders to further integrate the CISO role into the organization's leadership structure, thereby increasing the security, business utility, and resilience of organizational information technology (Karanja & Rosso, 2017).

Business Technical Problem

Determining what roles are critical for the success of the CISO within the U.S. federal government contracting organization is crucial to ensuring the security and resiliency of the government supplier (Karanja & Rosso, 2017). It is also essential to understand how the CISO integrates and interfaces within an organization’s information technology leadership team. An effective interface with IT leadership ensures that digital products and services effectively support mission requirements throughout the business and are delivered securely (Murphy, 2018). Additionally, it must be understood how the CISO integrates within the organization’s senior leadership team to appropriately manage organizational information security risk (Reagin & Gentry, 2018). While trade journal and magazine articles exist related to the chief information security officer's role, a significant gap in academic literature exists as it relates to the role (Karanja & Rosso, 2017).

The general problem under investigation is that government contracting organizations face the threat of not establishing new or maintain existing contractual work as a result of non-compliance with U.S. federal cybersecurity requirements. The specific problem is that executives within government contracting organizations do not understand how to strategically align the

CISO in the government contracting organization to support an enterprise digital strategy that includes U.S. federal government cybersecurity requirements.

Research Purpose

The purpose of this qualitative classical Delphi study is to identify the roles of the CISO in a government contracting organization as viewed by a panel of cybersecurity experts and to determine the extent to which there is a consensus of opinion among these experts related to the identified roles. No academic literature was identified related to the CISO role within government contracting organizations. Therefore, this study adds to the body of knowledge related to information technology and information security. This study's business/mission application is to facilitate government contracting leaders to better plan for, understand, and utilize the CISO role. Contractors will be able to better use the CISO as both a strategic and tactical leader to establish long-term plans and short-term protections that will result in a more resilient organization and information technology infrastructure.

A study related to the role of the CISO in the U.S. federal government contracting organization is very timely, considering the increasing focus of the federal government on supplier cybersecurity practices (DOD, 2019). This study serves to inform the executive leadership of government contracting organizations regarding the best way of integrating and utilizing the CISO as a critical business enabler. The ever-growing pace of digital transformation in our nation (Andriole, 2017) focuses on the need for information security and a clear understanding of the role of the CISO.

Research Question

Consensus does not exist related to the roles of the CISO in the government contracting organization in support of meeting U.S. federal government requirements related to cybersecurity. To this end, this study endeavors to answer the following research question:

RQ: To what extent is there a consensus among a panel of security experts as to the roles of the CISO as it relates to establishing and maintaining a government contracting organization's information and data security?

Rationale

Consensus does not exist related to the strategic alignment of the role of the CISO in the government contracting organization in support of meeting U.S. federal government requirements related to cybersecurity. Understanding how the CISO integrates strategically into the modernizing of a government contractor's technology landscape is critical to government contract leaders (Mithas & Rust, 2016). The CISO role must be appropriately placed within the organization to affect change from a technical protection perspective while also communicating with organizational leadership from a strategic planning perspective (Karanja & Rosso, 2017). The technology field is changing rapidly, especially when one considers technologies such as blockchain, artificial intelligence, robotic process automation, and quantum computing.

Consequently, this means that the role of the CISO must evolve to address advances in new technology (Wallden & Kashefi, 2019). The CISO role is becoming more strategic to drive mission value and to assist mission leaders in establishing an appropriate cyber risk posture for the organization (Hooper & McKissack, 2016). Understanding how these strategic mission roles that the CISO must exemplify is of critical importance to the CISO and to the organization’s utilizing a CISO as they choose how to implement the position within their organizations.

Conceptual Framework

Organizational culture (OC) theory contributes to the conceptual framework for this research. OC defines culture as the beliefs that a group of individuals possesses that have developed over time and are agreed upon by the group members to be valid. Organizational Culture is passed on to new members of the same group to perceive reality and respond to stimuli related to the activities of the organization and its members (Schein, 2017). For this research, OC is broken down into three levels that allow for further analysis of the data collected as part of this study's research. Figure 1 presents the three levels of organizational culture theory.

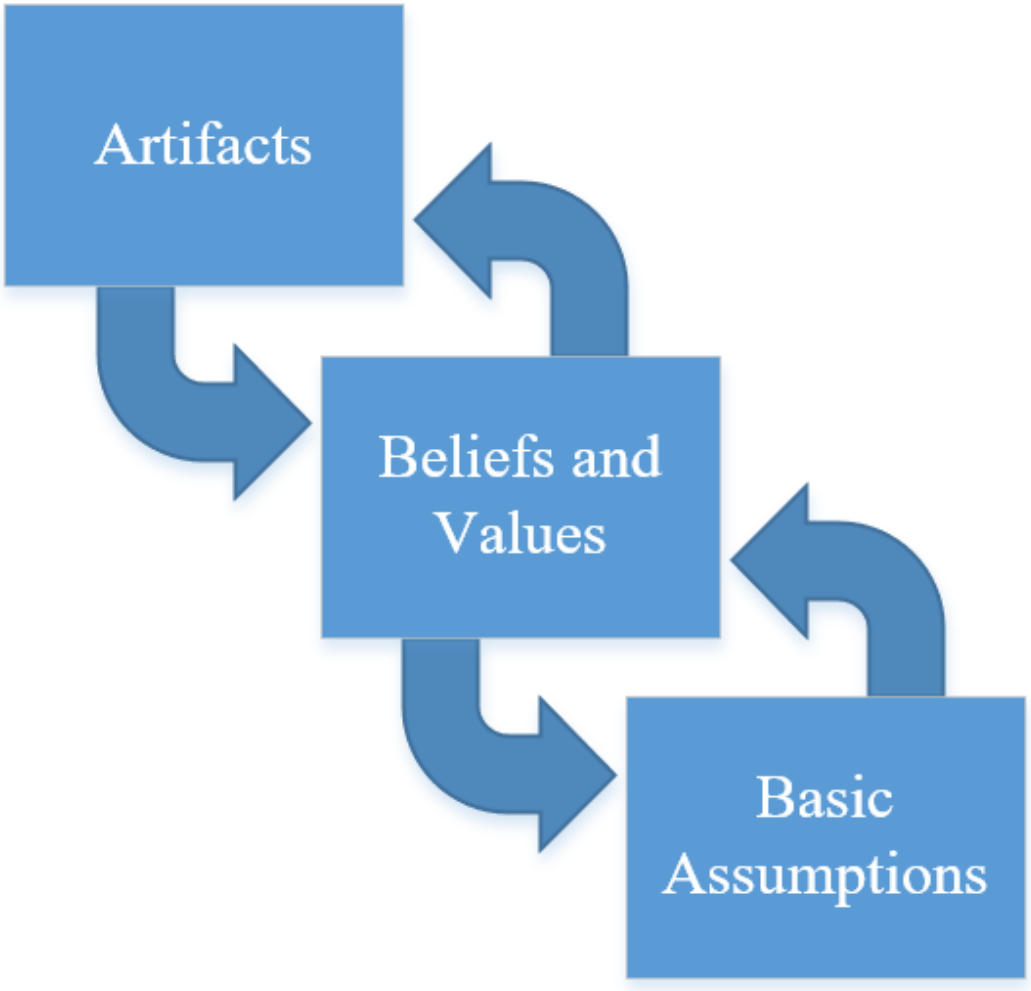

Figure 1. Levels of Organizational Culture (Schein, 2017)

The first level of organizational culture focuses on artifacts. Artifacts are those things that make up an organization and are associated with something that you hear, feel, and see. Examples of artifacts in this context include the types of physical workspaces, tools employed, artistic expressions such as corporate branding, legends about the organization, published ideals, and observed customs. The second level of OC deals with the beliefs and values espoused by the organization. This level relates to the organization's principles, objectives, measurements, specifications, and ethical foundations. The final level of OC theory discusses the underlying assumptions taken for granted to be valid within the organization. This OC theory level deals with the assumptions that the organization holds as true based on trial and error. Individuals determine which courses of action result in positive results over time and teach these actions to others. Because these behaviors are taken for granted, they can be challenging to measure as individuals within the organization may not recognize the behaviors (Schein, 2017).

Utilizing OC as a lens to examine the role of the CISO within the government contracting industry is appropriate since the CISO, as a business and information technology leader, must understand the organizational culture effectively to affect positive change from an information security perspective (Tang, Li, & Zhang, 2016). Additionally, as a change agent and business leader, the CISO must work to embed information security principles into the organizational culture helping all team members of the organization to understand their role in protecting the corporation (Murphy, 2018). Based on an understanding of Organizational Culture Theory and the need for leadership to manage and cultivate an effective organizational culture (Marinova, Cao, & Park, 2019), the CISO must work to establish an information security culture that aligns with and supports the organization’s culture (Tang et al., 2016).

Significance

This study is significant because strong information security leadership is required within U.S. federal government contracting organizations. In the October 16, 2019 publication of Cyberscoop, the synopsis of a presentation was published from Katie Arrington (Lyngaas, 2019). Katie Arrington is the chief information security officer of the Pentagon's acquisition policy office within the Department of Defense. This government representative informed the defense contractor community that the DOD's new cybersecurity compliance requirements must be implemented by the contractor community to win new contracts in 2021. In the same article, the government representative stated that the DOD understands that the requirements will cost money for their suppliers to implement and that this is necessary to secure the DOD supply chain (Lyngaas, 2019). These statements clearly show that the government takes its suppliers' security seriously and expects its suppliers to comply with essential federal cybersecurity standards related to contractor security. The need to comply with federal cybersecurity requirements raises the stakes for the CISO and the contracting firms they serve. The stakes are raised because cybersecurity compliance with U.S. federal government standards will be required to win future contracts. These cybersecurity standards help to provide the government with a mechanism to down select vendors that have not established a strategic cybersecurity program for their organization (Doubleday, 2019).

Understanding the role of the CISO is essential as the CISO plays a crucial role in supporting a government contracting organization's competitiveness by implementing supplier cybersecurity requirements directed by the U.S. federal government. It may present some areas of weakness in the management of information technology within an organization that should be understood by both technical and mission leaders (Stewart & Jürjens, 2017). Where the CISO

position needs to align in the future is incredibly important, especially considering the pace of technological advancement. Understanding this alignment will help supplier mission leaders plan appropriately and integrate the cybersecurity management function properly within their respective organizations (Granneman, 2018). Also, this study may serve as a guide for government contracting leaders to establish changes and controls within the reporting structures of the CISO in relationship to their C-suite and Board (Karanja, 2017) with the goal of better managing technology risks. Additionally, this study can be used as a starting point to conduct additional follow-on research related to current deficiencies seen in the CISO role. Finally, future studies can develop more comprehensive research related to individual skills that a CISO may need in the future related to expected changes caused by IT modernization and technical advancements.

The CISO is the single executive-level organizational leader that ensures that corporate information systems are managed in a secure and resilient way. The American public expects that their government is operated securely and that their personal information and social services are safe and resilient. The U.S. federal government is responsible for safeguarding the liberties of our nation. The government also is responsible for housing vital personal information related to every citizen. Finally, the government conducts operations and research that is highly sensitive that would be of great interest to a nation-state attacker allowing their nation to have a strategic advantage if our data was inadvertently disclosed. The U.S. federal government presents a large target for groups such as nation-states attackers and organized crime. Due to the large attack surface, the U.S. federal government presents, government contractors must secure their information technology infrastructures to reduce this threat surface from a third-party risk management perspective.

The nation-state attackers are highly funded and resourced through the backing of an entire country, making them highly formidable. Cybercrime enriches criminals in ways that have only been available in the modern era. Historically, a criminal would need to engage in dangerous activities to steal information or money. Criminals can now reach out across the Internet in relative safety to steal intellectual property and extort resources from organizations. The example of the Baltimore City data breach in 2019 in which ransomware caused significant disruption to city services, highlights the fact that cybercrime is a real threat to the government (Chokshi, 2019). This case is where ransomware took many critical Baltimore City information systems offline, rendering them unusable. In this case, the attackers demanded 13 bitcoins to re-enable the system, which was approximately $75,000.00 at the time of the demand. Organizations must ensure that they perform due care and due diligence related to their implementation of cyber hygiene principles. In doing so, an organization will be working towards ensuring that they are well protected and resilient against information security vulnerabilities and attackers that would wish to exploit those vulnerabilities.

Attackers do not tend to target organizations using highly sophisticated attacks. Instead, the attacker examines the target organization for apparent weakness that can be exploited (Verizon, 2019). Considering that the attacker can utilize less sophisticated means to attack an organization, a need to focus on the concept of cyber hygiene presents itself (Cain, Edwards, & Still, 2018). Cyber Hygiene is the concept that an organizational information system can be unhealthy and that basic practices can be implemented to ensure its health. Some of these information security practices include effective patching, implementing strong standards and baselines, and establishing a complete inventory of devices. In most organizations, the IT operations team implemented these and many other practices but independently verified and

validated by the cybersecurity team. The CISO role's significance is magnified by the above examples of information system configurations and the attackers that would wish to exploit misconfigurations.

Cybersecurity attacks are continuously in the news because shortcuts are made in information security procedures, leading to organizational or client information exposure. In May of 2017, an employee of Booz Allen Hamilton insecurely configured an Amazon Web Services (AWS) data store leading to the disclosure of 60,000 sensitive records being exposed that belonged to the U.S. National Geospatial-Intelligence Agency (NGA; O'Neill, 2017). In May of 2019, Equifax had its credit rating downgraded from stable to negative (Fazzini, 2019) due to a breach in 2017 (Bernard, Hsu, Perlroth, & Lieber, 2017). This event is important for several reasons. First, this is a historic event in that an organization's credit rating has been directly affected based on a cyber incident. In the past cyber incidents were understood only to have a short-term effect on an organization's overall market performance (Lange & Burger, 2017). The downgrade in Equifax's credit rating is the first time a cyber event has directly affected a large organization's potential long-term market performance by influencing the firm's ability to access credit. Second, this event allows us to remove fear, uncertainty, and doubt (FUD) from the cyber conversation related to specific cybersecurity mismanagement consequences.

Definition of Terms

The information provided in this section serves as a reference to the reader related to critical operational terms contained in this dissertation.

Chief Information Security Officer: The chief information security officer (CISO) is the technology leader responsible for developing, implementing, and managing an organization's

information security program (Karanja, 2017). The way the CISO role is implemented can vary widely depending on the organization (Hooper & McKissack, 2016). Some organizations may implement the CISO role as an IT security manager within an IT organization. In contrast, others may implement the CISO role as an executive function that reports to an organization's Chief Executive Officer (Hooper & McKissack, 2016).

Cybercrime: Cybercrime is where criminals utilize information technology assets to conduct scams against public and private institutions with the goal of financial gain. Cybercrime is a global multibillion-dollar a year criminal enterprise that is not confined to a single nation's boundaries (Whissemore, 2018).

Cyber Hygiene: Cyber Hygiene is the concept that an organizational information system can be unhealthy and that basic practices can be implemented to ensure information systems health. In most organizations, these and many other practices are implemented by the IT Operations team but independently verified and validated by the cybersecurity team. Some of these information practices include Effective Patching, implementing strong Standards and Baselines, and establishing a complete inventory of devices. (Cain et al., 2018).

DFAR 252.204-7012: Defense Federal Acquisition Regulation (DFAR) Supplement 252.204-7012. This guidance requires Defense Department contractors to implement the controls defined in NIST SP 800-171 (Sweeney, 2018).

Nation-State Attacker: Nation-State attackers are cyber teams that utilize the resources of an entire nation to conduct offensive cybersecurity operations (Coburn, Leverett, & Woo, 2019). In this case, the attacker has incredible access to technical tools, human resources, and funding to conduct cyber operations that are advanced and difficult to detect.

National Institutes of Standards and Technology (NIST) Standard Publication (SP) 800-171: NIST SP 800-171 establishes the security standards and guidance related to protecting federal government contractor information systems (Ross et al., 2018).

Ransomware: Malicious software is used to prevent access to an information system to extort money from an organization. The attacker demands a ransom from the victim, claiming access to the information system will be allowed once the ransom is paid. (Zimba & Chishimba, 2019).

Cybersecurity Maturity Model Certification (CMMC): The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity framework and certification model that is designed to increase the security of the Defense Industrial Base (DIB). This standard is needed because the DIB as a supplier to the Department of Defense (DoD) can be used as a vector for entrance into the DOD networks. Additionally, as sensitive information may reside on supplier networks, an adversary can target these networks to exfiltrate this sensitive information without ever attempting to enter the DOD network (Doubleday, 2019).

Organizational Culture: Organizational culture is also the shared beliefs and assumptions held by the individuals who make up the organization. Culture as a concept can be viewed as the ideological, symbolic, and abstract expressions that make up individual communities (Schein, 1992).

Information Security Culture: Information security culture is how employees view their role regardless of rank as it relates to protecting the organization from security threats (Tang et al., 2016). Information security culture and organizational culture influence each other leading to positive security outcomes when managed effectively (Santos-Olmo, Sánchez, Caballero, Camacho, & Fernandez-Medina, 2016).

Risk Management: The effective identification, documentation, triage, and minimization of enterprise risks that may impact an organization's ability operate in a resilient fashion in accordance with mission requirements (Ogutu, Bennett, & Olawoyin, 2018).

Assumptions and Limitations

Assumptions

This study assumes that the expert panel participants did not falsify their credentials and possessed the necessary background and experience to participate in the study. Further, it is assumed that the study's participants have an expert understanding of developing, implementing, and managing an organization's information security program. Additionally, this study assumes that all participants were truthful in their answers and did not attempt to improve the appearance of their roles by answering dishonestly to any study-related questions.

Limitations

This study was limited to information technology and information security leaders currently serving or have served in the CISO role for U.S. federal government contracting organizations. For those currently not serving in the role of CISO, a time limit of 5 years was imposed. As part of this 5-year time limit, individuals must still be actively involved in the information technology and information security communities in the GovTech space. Anyone that falls out of this 5-year range was not included in the studies population. The specific roles allowed to be part of this study include the CISO, Chief Information Officer (CIO), and any similar roles to the CISO, where an organization may utilize an alternative naming convention for the role. The study scope was limited to just U.S. government contracting organizations. As a result, other industries and focus areas were not addressed as part of this study's research.

Organization for Remainder of Study

As part of this first chapter, the following topics were discussed: introduction, background, business technical problem, research purpose, research question, rationale, conceptual framework, significance, definition of terms, assumptions and limitations, and organization for the remainder of the study. This dissertation consists of four remaining chapters. Chapter 2 is the literature review where available research on the topic being studied is reviewed (Dahlberg & McCaig, 2010). Chapter 3 presents the design and methodology, participants, setting, analysis of research question, credibility and dependability, data collection, data analysis, and ethical considerations. Chapter 4 discusses the study's data collection and analysis results. Chapter 5 contains the evaluation of research question, fulfillment of research purpose, contribution to the business technical problem, and future research recommendations.

CHAPTER 2. LITERATURE REVIEW

Introduction

This chapter provides a thorough and complete review of the available literature on the role of the chief information security officer (CISO) and U.S. federal government cybersecurity requirements and synthesis of resources related to the more general field of information security management. The remaining sections of this chapter include Methods of Searching, Conceptual Foundation for the Study, Review of Literature, and an Overview of Research Findings. The methods of searching section describes the sources and mechanisms that were used to gather the information that was used as part of the literature review. The conceptual foundation of the study sections reviews and aligns the conceptual framework of the study into the topic being researched. The review of literature section synthesizes the available literature related to the role of the CISO and information security management to understand what is known about the business problem under investigation. This section contains five sub-sections which thoroughly analyzes the role of the CISO and how the role integrates into the mission of the US federal government contraction organization. The literature review subsections are Changes in the federal government's Focus on Cybersecurity, The CISOs Role Related to Business Integration, The CISOs Role Related to Technology Integration, The CISOs Role Related to Data Protection, and The CISOs Role Related to Information Security and Risk Management. The Synthesis of Literature section synthesizes and summarizes the research findings of the literature review and provides a critique of the research methods used in the reviewed literature.

Methods of Searching

Several sources and search mechanisms were used to support this literature review. Scholarly articles and trade publications were used to develop an understanding of the research

that was being developed in this area. These sources allowed for a thorough review of what scholars and practitioners were experiencing and addressing. The search tools used to discover the literature for this review included google scholar, google, and the Capella Library databases. Specific databases used within the Capella Library include Business Source Complete, which was used to curate business and management articles. These articles related to the integration of information security functions into the business from a strategic perspective. The Computers and Applied Science database was utilized to focus searches on information technology specific articles. In support of methodological research, the SAGE Research Methods database was used to support the research related to this study's Delphi methodological approach.

This literature review provides a decomposition of the available literature related to the role of information security and information technology leadership from various sources to include scholarly journal articles, books, practitioner related media, U.S. federal government standards, guidance, and regulations, and industry research. The *search terms* used to discover the resources in this literature review include *chief information security officer, CISO, Information Security Management, Information Security Manager, Chief Information Officer, CIO, IT Security Manager,* and *IT Security Management*. While the literature search yielded many valuable results related to information security management, there is very little current scholarly literature pertaining to the role of the CISO. The lack of academic data on the role of the CISO was identified through database searches in support of this literature review and a review of the scholarly research available about the CISO role (Karanja & Rosso, 2017).

Relevance of Conceptual Foundation

This study's conceptual foundation is tied to the conceptual framework identified in Chapter One and the seminal work developed by Edgar Schein related to organizational culture.

Foundationally organizational culture theory is the shared beliefs and assumptions held by the individuals who make up the organization (Schein, 1992). Culture as a concept can be viewed as the ideological, symbolic, and abstract expressions that make up individual communities. The quintessential aspects of culture are not defined by the tangible artifacts present in a community of individuals. Instead, culture is determined by how the group members, through their shared information, knowledge, and characteristics, utilize the tangible aspect of the culture and interact with one another (Banks & McGee-Banks, 1989). From an organizational culture perceptive, culture concepts are applied across an organization at the enterprise level down to the line team member to solve internal and external problems related to mission performance (Schein, 1992). Schein observed that it is the responsibility of organizational leaders to ensure that the culture is not developed organically through ad-hoc interactions. Instead, organizational culture should be developed in a methodical manner where leaders establish and adjust corporate culture to ensure positive organizational outcomes (Schein, 1992).

Schein believed that organizational culture theory could be broken down into three levels that allow for further analysis of an organization and how its culture affects its ability to be successful. The first level has to do with organizational artifacts. Artifacts are those things that make up an organization and are associated with something that you hear, feel, and see. Examples of artifacts related to organizational culture theory can include the types of physical workspaces, tools employed, artistic expressions such as corporate branding, legends about the organization, published ideals and observed customs. The second level of organizational culture theory has to do with the beliefs and values espoused by the organization. This level relates to the organization's principles, objectives, measurements, specifications, and ethical foundations. The organizational culture theory's final level discusses the basic assumptions taken for granted

to be valid within the organization. This level of organizational culture theory deals with the assumptions that the organization holds as true based on trial and error. Individuals determine which courses of action result in positive results over time and teach these actions to others. Because these behaviors are taken for granted, they can be challenging to measure, as individuals within the organization may not recognize the behaviors (Schein, 1992).

Schein established that organizational culture theory allows the researcher, observer, or organizational leader to understand the nature of an organization, whether the organization is operating well or even when the organization is dysfunctional (Schein, 1992). Through this understanding, the shared beliefs and assumptions that define a group can be better understood as the set of norms that the group uses to set themselves apart from other groups and establish meaning related to their place in the group. Schein described the organizational leader's role as responsible for establishing and maintaining the desired culture for the organization (Schein, 1992). The organizational leader establishes an organization's culture as new groups of people are assembled to perform a needed function. The leader sets these new groups' expectations through active management to produce positive outcomes for the organization. When the leader does not actively manage the group, a culture will develop organically. This culture may be detrimental to the organization if it does not align with the enterprise's overall organizational culture (Schein, 1992). An ineffective organizational culture can lead to many problems within an enterprise. Weak cultures can lead to lower quality deliverables, increases in safety incidents, and higher employee attrition (Fletcher & Jones, 1992). This is why the organizational leader must be actively engaged in setting the culture for newly established groups and maintaining a healthy culture for groups as they operate.

In cases where organizational culture does not meet the needs of the enterprise, it is the responsibility of the organizational leader to step in, dismantling the ineffective culture and implementing new policies, processes, and procedures that support the positive outcomes that the organization is seeking to generate (Schein, 1992). This process of establishing a new culture, whether it is related to newly developed or already established groups, was identified by Schein to be a time-consuming and challenging process. As organizational culture is the shared beliefs and assumptions that are held by the individuals that make up the group being managed, the leader must ensure that they are working effectively with their team to build a culture that can be adopted by the group. Organizational culture can be established within an enterprise based on many factors and phenomena (Schein, 1992). As previously mentioned, culture can arise organically and unintentionally through individuals' natural interactions within an organization. Examples of where unintentional organizational culture can appear are when new organizations are established or exiting organizations are merged, forming a new organization without a strong leadership presence. In this case, these organizations' group members will establish a culture based on their shared beliefs and norms about the organization and their place in the enterprise (Cameron & Quinn, 2006).

Intentional culture is established when leadership defines and promulgates the values that have meaning throughout the organization in a systematic and planned manner. The values that the leader instills in the organization will become part of the group's shared experiences serving to reshape organizational culture (Boggs, 2004). This process of cultural change management within the group takes time to implement, as the team must accept the new culture and incorporate it into their commonly held beliefs. To be conducted effectively, this takes time and trust from both the organizational leader and the team members that are being led (MacIntosh &

Doherty, 2009). Understanding how to manage and shape organizational culture is a critical skill required to advance and mature an organization (Schein, 1992). Since Schein's seminal work on the topic of organizational culture, scholarly research has been conducted that presents evidence for how organizational culture influences the enterprise and the team members that make up the groups that support the enterprise's mission. Additional studies exist that support the conclusion of Schein and show that an effective and business-aligned organizational culture can contribute to organizational success (Cameron & Quinn, 2006), greater employee fulfillment (McIntosh & Doherty, 2009), and improved project and deliverable quality (Boggs, 2004).

Organizational culture theory is an essential tool that can be applied in understanding how human behaviors are influenced and impacted in the enterprise. Through rigorous scientific review, organizational culture theory has been demonstrated to have a measurable impact on the performance of an organization (Schein, 2017). Organizational culture is critical to understand as it relates to effectively interacting with the organization from an Information Technology and Information Security perspective. The values that are shared and championed throughout the organization will directly impact technology and security management effectiveness.

Organizational culture is significant in developing and sustaining an effective information security program (Tang et al., 2016). Additionally, information security leadership in the form of the chief information security officer directly affects and influences organizational and information security culture to develop and lead information security program development. When designing the information security program, the CISO must be keenly aware of the impacts that the security program will have on the organization and the groups of people that make up the organization (Li et al., 2019). The individuals who make up the organization are critical to the success of the information security program and the organization's overall security

posture. Regardless of an individual's position in an organization, everyone has a role to play in establishing a secure organization, whether they are senior executives, middle management, or line staff (Kennedy, 2016). Line staff is responsible for processes that include securely conducting their business activities, while also notifying responsible individuals if they see something suspicious that could lead to an information security incident. Securely conducting their activities would include activities like not downloading software from untrusted sources or clicking links in an email that could lead to business email comprise (Goel, Williams, Dincelli, & University at Albany, 2017). If an employee discovers suspicious behavior where they are concerned that organizational security is compromised, the process for reporting an incident should be executed. This allows the organization's response team to be mobilized so that a potential incident can be investigated and mitigated if needed. (Cain et al., 2018).

The middle manager is responsible for activities that include ensuring employees adhere to corporate information security policies and that all projects undertaken by their teams include information security as part of project initiation (Kulkarni, 2018). By ensuring that their team adheres to information security policy, the manager helps maintain the organization's resilience by ensuring that all team members do their part to ensure a secure enterprise (Kennedy, 2016). By including information security at project initiation for all technical projects, that manager ensures that security is built into their division's projects. Which further drives resiliency and a reduction in overall project costs due to eliminating potential re-work and incurred technical debt due to missing security controls (Sabherwal et al., 2019).

Senior executives set the tone for the information security program by establishing support and a clear need for information security throughout the organization (Rothrock, Kaplan, & Oord, 2018). By setting the need for information security within the organization, the

executive leader is tying the information security program and information security culture to the enterprise's organizational culture. This helps organizational team members understand the importance of information security for the organization and helps them understand the priority placed on it by organizational leadership (Tang et al., 2016). A key component of orchestrating the senior executive, middle manager, and line staff's roles and responsibilities are effective role-based communication, awareness, and training related to information security (Kennedy, 2016). Implementing this capability allows the CISO to shape organizational and information security culture by training employees on their needed responsibilities to do their part in ensuring that the enterprise is secure against modern threats and attacks. The communication, training, and awareness capability implemented by the CISO in support of organizational and information security culture change serves to provide the needed information to team members based on their role within the organization (Hooper & McKissack, 2016). Providing this capability ensures that team members know exactly what they need to do and why they need to perform an action to protect an organization. In performing this capability, the CISO is promulgating new organizational and information security culture to ensure an enduring and resilient enterprise (Karanja, 2017).

Organizational culture theory applies to this research as this research attempts to identify the role of the CISO within the government contracting industry. The CISO, as a business and information technology leader, must be able to understand, manage, and change organizational culture effectively throughout an enterprise to affect positive change from an information security perspective (Tang et al., 2016). Additionally, throughout the organization, the CISO works to define and integrate information security principles (Whitten, 2008). Understanding organizational culture theory and the mechanisms needed to implement change with high

adoption rates are necessary for the CISO to be successful (Murphy, 2018). As such, it is the responsibility of the CISO to establish an information security culture that supports the organization's mission (Tang et al, 2016) from a risk management perspective while also working to modify organizational culture and employee behavior (Marinova et al., 2019). Understanding organizational culture theory helps in better understanding the observations made during data collection. A group of industry experts was assembled to describe the roles needed for the CISO within the government contracting space. The CISO is a senior leadership position and organizational change agent role within an organization (Lanz, 2017). As such, an understanding of organizational culture theory allowed the panel of experts' responses to be analyzed through the lens of organizational culture theory. This allowed for greater clarity and context when drawing meaningful conclusions from the analyzed study data.

Current and developing standards exist related to securing U.S. federal government contractor information systems against cyber-attacks (Dombora, 2016). These standards have been developed mainly to ensure that sensitive government information being stored on contractor information systems is protected from misuse and fraud. Standards like the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171 (Ross et al., 2018) and the Cybersecurity Maturity Model Certification (DOD, 2019) from the Department of Defense are designed to ensure a safe contractor operating environment where government information can be stored. The business problem under investigation as part of this study is that government contracting organizations face the threat of not establishing new or maintain existing contractual work because of non-compliance with U.S. federal cybersecurity requirements. Understanding organizational culture theory provides a better understanding of the business problem under investigation as part of this study. The business problem requires the CISO to

serve as a change agent within their respective organizations developing effective strategies that support creating a robust information security culture and effectively change the enterprise's organizational culture. The organizational culture changes within a government contracting organization related to U.S. federal government cybersecurity requirements will require the CISO to make a clear case for cybersecurity capabilities as a means for the company to invest in cybersecurity, which will lead to continued work and revenue (Death, 2019).

In the December 16, 2019 publication of Breaking Defense, an interview was published with Major General Thomas Murphy. He is the Protecting Critical Technology Task Force director within the Department of Defense (Freedberg, 2019). As part of this interview, Major General Murphy discussed that if contractors were unable to meet the Department of Defense's cybersecurity requirements, they would not be able to compete for future contracts (Freedberg, 2019). Major General Murphy also described a situation where their suppliers' lack of security had created an environment where the Department of Defense can have its mission compromised by the inaction of its selected suppliers (Freedberg, 2019). Security vulnerabilities being introduced via DOD suppliers is seen as an unacceptable proposition by the Department of Defense. The DOD will address its vendors' cybersecurity requirements by implementing the Cybersecurity Maturity Model Certification (Freedberg, 2019). Major General Murphy explained that if a contractor could not meet the certification level for a specific contract, the contractor would be barred from bidding on that particular contract (Freedberg, 2019). These realizations would be devastating to a government contractor's business that relies on the Defense Department as a source of revenue. With the Cybersecurity Maturity Model Certification standard and the information provided by Major General Murphy, a clear case can be made by the government contractor CISO to establish a business-focused information security

program. The security program would support business resilience and the organization's continued ability to compete for and win government contracts (Karanja, 2017). Successful information technology projects are associated with technology leadership that aligns a given technology project with the mission of the organization (Sabherwal et al., 2019). In this case, it will be the role of the CISO to work with organizational leaders to actively change the enterprise's organizational culture in support of an enhanced cybersecurity posture (Hooper & McKissack, 2016). Adapting the organization's culture will be supported by the organization's clear and present need to meet the contracting requirements of the government, making this change in organizational culture directly tied to the mission of the enterprise (Cameron & Quinn, 2006).

Understanding how to develop a healthy organizational culture is essential for the enterprise as culture is critical in creating a dynamic and effective organization (Browning, 2018). As part of understanding the development and implementation of an effective organizational culture strategy, it is essential to understand that cultural aspects can exist at various levels within the organization (Schein & Schein, 2019). At the highest-level, culture is developed and championed by executive management across the enterprise. This cultural tone establishes the norms that are expected throughout the organization. Throughout the organization, a culture will also be established as part of the various groups that make up the company (Schein, 2017). As an example, the culture that defines the financial management organization led by a corporate Chief Financial Officer may have a very different culture than a Human Resources division led by a Chief of Human Capital. As the two organizations have very different missions, natural, cultural differences will become apparent over time. The financial organization will be highly focused on corporate performance and investment return that a

technological advance brings to the organization (AICPA, 2018). Human resources (HR) will be focused on supporting organizational team members. HR's focus on technological capabilities will align with how new technology supports the HR division's goals related to employee services and corporate compliance (Armstrong, 2017). The two examples of Finance and HR, while having culture components of their own, also inherit the enterprise's cultural attributes either through careful planning by executive leadership or organically as part of the shared experiences of the human community that makes up the organization (Schein, 2017). An organization where executive leadership carefully plans and shapes its organizational culture is more successful than organizations that have simply allowed a culture to form overtime without planning and direct management intervention (Pettigrew, 1979).

When management does not intentionally focus on organizational culture, a culture will develop in the void. An ad-hoc culture will grow in this case because people establish culture as part of their community, which in this case, is the workplace. As individuals interact, they will begin to develop beliefs and biases about the organization and its members. Suppose organizational leadership does not work to ensure that a defined culture is established. In that case, they will inherit an organically developed culture that may or may not benefit the organization's effectiveness and resiliency.

Review of Literature

There has been an increased focus on the role of chief information security officer in recent years and the skills needed to perform the information security management leadership function for an organization (Haqaf & Koyuncu, 2018). While there has been a significant focus on the CISO role from a popular and trade article perspective, there has been little academic research on the topic (Karanja & Rosso, 2017). As limited academic research exists on the

subject, this provides an excellent opportunity to provide meaningful research analysis to further the overall body of knowledge related to information technology management. As digital systems have proliferated across government contractor enterprises, the need to protect sensitive governmental information on those systems has become a priority (Doubleday, 2019). The CISO and technology leadership role in safeguarding mission execution, identifying risk, and supporting mission success has become critical in ensuring organizational resiliency (Griffy-Brown, Lazarikos, & Chun, 2019). For the government contracting organization, the need to protect governmental and sensitive information has fostered a close relationship between the organization's business units and the CISO (Trope, 2018). As the CISO works to develop the organization's information security program in partnership with the business, critical aspects of the organization will be addressed related to how technology is used and how data is protected within the organization.

As government requirements have begun to mature related to supplier security, it is apparent that the government is starting to take the technical controls implemented by its vendors much more seriously. The U.S. federal government has developed and promulgated standards to ensure sensitive governmental information residing on government contractor digital systems are safeguarded (Ross, et al., 2018). Measures like these are designed to motivate the government contractor community to make more secure choices related to their implementation of information systems that support U.S. federal contracts (Reagin & Gentry, 2018). The lack of academic research into the role of the CISO, coupled with the increased focus provided by the U.S. federal government related to contractor security, offers an excellent opportunity to focus on the role of the government contractor CISO as an area of study.

Information technology plays an ever-increasing role in mission execution due to the value that information technology brings to mission delivery (Mithas & Rust, 2016). Because of the great value that information technology brings to the organization, its proliferation has increased at an ever-increasing rate (Griffy-Brown, et al., 2019). Due to the expansion of digital systems across government contractor enterprises and the need to protect sensitive governmental information on those systems (Trope, 2018), the U.S. federal government has begun to deploy standards designed to safeguard confidential government information on contractor digital systems. These standards provide motivation and guidance for organizations to follow when implementing security controls throughout their organization's enterprise (Reagin & Gentry, 2018). The CISO is the single individual charged with ensuring that organizational systems meet federal cybersecurity requirements and that these requirements are met securely. This focus area will gather research into how the CISO is being used and is aligned within the U.S. federal government Contracting Industry.

Changes in the Federal Government's Focus on Cybersecurity

The role of Cybersecurity and the CISO is receiving better support with significant resources being applied to planning for and implementing security protections for information systems as a result of cyber-attacks and increased cybersecurity requirements on businesses (Rothrock et al., 2018). From both a legislative and company leadership perspective, cybersecurity and privacy concerns are being given focus across federal government agencies (Brekke & Cassidy, 2019). The U.S. federal government, from a leadership perspective, has been pouring significant resources into their internal cybersecurity posture. The U.S. federal government has made significant efforts since 2016 to develop information security standards

that effectively support the information protection requirements of the government related to securing sensitive government information residing on contractor networks.

In 2016 an inter-governmental CISO role was implemented during the Obama administration to spearhead a strategy focused on implementing safeguards within federal agencies and fostering information sharing across agencies related to cybersecurity (Scott & Daniels, 2016). Additionally, the National Institutes of Standards and Technology (NIST) released the Special Publication (SP) 800-171 in 2016 titled: "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (Ross et al., 2018). This document contained information security controls that the federal government considered necessary for government contractors to implement to safeguard sensitive government information residing on contractor networks. In 2017, the Department of Defense released guidance as part of the Defense Federal Acquisition Regulation (DFAR) Supplement 252.204-7012. This supplement required defense contractors to implement the security controls outlined in NIST SP 800-171 (Sweeney, 2018). In 2018 the Cybersecurity Infrastructure Security Agency (CISA) was established to spearhead cybersecurity protections in the federal government and act as a partner with the private sector to protect critical infrastructure and vital United States intellectual property and critical infrastructure assets (Whitehouse.gov, 2018). The FISMA Act (Carper, 2014) and its corresponding agency-level analysis and reporting (Yimam & Fernandez, 2016) require that agencies understand their information systems' cybersecurity posture and report that posture outside of their agency for review and analysis. In 2020 the U.S. federal government is imposing barriers to entry related to security requirements as part of the contractor solicitation and acquisition process for U.S. federal contractors (Brekke & Cassidy, 2019). Additionally, this presents a new reality of continuous compliance management for the

contracting organization as these compliance requirements continue to mature for the contracting organization.

The Department of Defense has released a standard/maturity model in 2020 called the Cybersecurity Maturity Model Certification (DOD, 2019). This standard will take the self-certified security attestation of NIST SP 800-171 and bring forth an external third-party verified maturity model that reports a contractor's security posture to the DOD (Doubleday, 2019). This new model will directly affect a contractor's ability to win contracts and ultimately result in contractors being unable to compete if they do not comply with the new standard. In addition to the Department of Defense changes, NIST will be introducing a new supplement to the 800-171 standard titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High-Value Assets" (Ross et al., 2019). This standard is applied to organizations that store and process extremely critical U.S. federal data.

These tools provide government contractor organizations with the necessary information to formulate their risk-based approaches to securing their information systems commensurate with the value of the data residing on those networks following government requirements (Dombora, 2016). The significant takeaway related to these changes to U.S. federal guidance related to information security is that the CISO must stay engaged with the ever-changing and evolving release cycle of information security standards. The CISO ensures that proper attention and focus are applied within the organization to new rules as the government releases them. By being keenly aware of changes, the CISO can ensure that strategies and priorities are updated to address new governmental requirements. These new requirements and policy changes will require close alignment with organizational leadership as any change of this magnitude will also

require top leadership commitment and funding (Granneman, 2018). The CISO is the leadership role that can bridge the gap between the government's compliance requirements and the organization's business and mission needs (Karanja, 2017).

The CISO's Role Related to Business Integration

The Chief Information Security Office role has risen to great prominence in the public sector. Understanding how the role operates today and how it should operate optimally is of great importance. Additionally, understanding how the role will change over the coming years with the push for information technology modernization and new advanced technologies will be critical to understanding how the CISO will integrate within the organization and what sort of services a CISO's information security program will provide to a government contractor. The contractor CISO's role in the area of U.S. federal government compliance is vital to the successful implementation of cybersecurity practices within the contracting organization. To establish a mission-focused and robust information security and risk management program for an organization, a strong leader must be in place to champion and manage the program (Murphy, 2018). The chief information security officer serves as the organizational leader who seeks buy-in and support from executive organizational leadership and team members' organizational-wide regardless of their position in the company (Cain et al., 2018). The role that the CISO plays with business executives in the government contracting industry is related to building support for the implementation of a successful strategy that will ensure a resilient and robust company that takes information security risk into account in accordance with the organizationally defined and maintained risk appetite (Ogutu et al., 2018).

Outside of executive management, the CISO works throughout the company to ensure that effective organizational change management techniques are employed. These techniques are

integrated into information security and core business functions (Kulkarni, 2018) and ensure that all corporate team members understand their role in maintaining a resilient, secure, and risk-managed organization (Cain et al., 2018). As a leader, the CISO must be well versed in all the operating capabilities of the business. For the CISO to be highly effective, they should not focus only on information technology problems (Haqaf & Koyuncu, 2018). The relationship that the CISO builds and fosters throughout the organization helps develop and sustain a sufficient understanding of its risk appetite (Ogutu, Bennett, & Olawoyin, 2018). Understanding the organization's risk appetite allows the CISO to prioritize better information security investments commensurate with the level of risk the business finds satisfactory (Granneman, 2018). This prioritization ensures that the most critical and necessary security controls are implemented before less important controls (Caldwell, 2017). Information security compliance has become common for the government contracting community and has become a cost of doing business (Granneman, 2018). As the government contracting community works with the federal customer to understand the government's security requirements, it is readily apparent that these new operating conditions will require effort and resources from the contractor community to implement (Ross et al., 2018).

While the CISO role and the requirement for cybersecurity are needed within contractor organizations, a review of the government contracting space reveals a significant fragmentation within the CISO role across and within a contracting organization. A review of job application sites like LinkedIn and Monster.com shows that roles with the title of CISO or similar can have very different job authority depending on the organization and the alignment of the organization's CISO role. It has been observed that a CISO’s salary can range between $127,000 - $235,000 for CISO roles in the Delaware, Maryland, Virginia Area (Payscale.com, 2019).

Additionally, the role that the CISO fills can be dramatically different with titles ranging from Director to Executive Vice President (Karanja & Rosso, 2017). The difference in these position placements is essential as the authority and organizational alignment differences can be significant. The literature has discussed that the CISO role should be an executive role directly influencing strategic planning processes (Hooper & McKissack, 2016). The CISO is also responsible for the organization's internal audit and information system security (Steinbart, Raschke, Gal, & Dilla, 2018). Care should be taken when placing the CISO in a role that may cause a conflict of interest with technology management divisions (Choi, 2016).

The role of the CISO will be changing in the future. An expected change area is related to CISO realignment within the organization to ensure executive leadership integration (Karanja, 2017). Another area of growth to consider is the establishment of new skills needed to manage an ever increasingly complex portfolio of new and innovative technology (Wallden & Kashefi, 2019). It will be the responsibility of the CISO to plan for a very different future environment. Based on the changes currently in the government contracting community around IT modernization, utilization of shared and third-party services, and the use of advanced technologies, the CISO will need to adapt to an ever-changing technical landscape. IT Modernization will continue to bring new technologies and information systems that the CISO will need to provide security services for, in concert with already existing legacy systems (Granneman, 2018). Shared and third-party services will require the CISO to open internal information systems to other external entities requiring shared interconnections and trust between organizations (Plachkinova & Maurer, 2018). Finally, new technologies implemented over the next decade will significantly change how the CISO conducts its business organizationally and within its information security program (Wallden & Kashefi, 2019).

The CISOs Role Related to Technology Integration

Historically, including the information security team in the initial activities of a project has been challenging across organizations (Kulkarni, 2018). There are many reasons for this, such as the appearance of security programs slowing down project execution, or security programs being seen as the organization that denies access to technology rather than finding a solution for business requirements. To address the problem of security being seen as a project delivery impediment, the CISO works with organizational business divisions to ensure that the information security program is well integrated into the needs of the business and their technology needs. The information security program should be well integrated into the organization's Systems Development / Engineering Life Cycle (SDLC / SELC) (Kulkarni, 2018) being brought into project discussion as early as possible. The earliest stage in a typical SDLC/SELC process is project initiation (Death, 2017). At this stage, the business customer is developing the mission requirements for new technical capabilities that are being proposed. During this stage, the CISO should inject security requirements into the project and advise mission leaders on protecting mission operations. The CISO will also be discussing how these protections serve to ensure continued mission and organizational resiliency (Karanja, 2017). By discussing security requirements at the earliest phase of a technology project, the CISO ensures that security is designed into new technological capabilities and not bolted onto technical solutions at a later time. Shifting to the left of the SDLC also provides that the organization is not accruing technical debt throughout the development and implementation of a new project (Granneman, 2018). From a security perspective, technical debt accrues on an IT project, the longer that security requirements and architectural principals are not applied to the design process. Early in the project life cycle, security requirements must be introduced, and those

requirements must be technically implemented through the design process. However, once the system has been designed, it can become very costly to retrofit, repair, or replace faulty design parameters (Granneman, 2018).

Additionally, a bolt-on security solution designed to protect a faulty component may not adequately protect the new system in a way that a designed-in approach would have done. When technical debt accrues against an information system, impacts will occur from both a monetary and an organizational risk perspective. The CISO collaborates with information system project teams to develop project life cycle gates that support the organization's appetite for risk (Ogutu et al., 2018) while ensuring that timelines for mission deliverables are maintained. Engaging with the organization will help alleviate the assertion that security slows down business processes. As a stakeholder in the process and as an adequately integrated project team member, the CISO can ensure that security requirements are integrated into the project and that critical timelines include security requirements, design review, and testing. The CISO, as a technological partner with the organization, must be customer service oriented and focused on ensuring that the mission has the tools that it needs to do its various jobs. The CISO partners with the business by ensuring that standards, guidance, and consultation related to information security are provided to the company in the form of effective security advisement (Karanja & Rosso, 2017).

Security advisement services provided by the CISO support the organization's information technology development and implementation capabilities while also extending into the ongoing operations of an information system and one-on-one consultations with organizational business units (Hooper & McKissack, 2016). The CISO supports the organization by developing solutions to technical security problems versus merely saying that a mission requirement cannot be accomplished. As part of an integrated project team, the CISO works with

the business to develop secure solutions to mission problems and develop alternatives when a selected business technical solution poses a risk to the organization. When developing secure solutions to a business problem, the CISO works throughout the SDLC process gates. In doing this, the CISO ensures that a solution has the correct security requirements and that these controls are securely designed. Once these controls are developed, the CISO ensures the controls are tested to ensure they operate as expected and that these controls do not undermine the information systems' performance. Finally, the CISO validates that the final production system is implemented as expected through a final validation process of production security controls (Death, 2017).

Once an information system is in production, the CISO will support the business through continuous diagnostics and monitoring. As part of this process, the CISO will ensure that the information systems stay configured in a secure state through periodic technical tests and manual audits (Karanja, 2017). These capabilities will help ensure that the system operates within the organization's expected risk tolerance and commensurate with the value of the data contained within the information system (Ogutu et al., 2018). Once a system has reached the end of its useful life, the system must be decommissioned securely. The CISO will work with the business and IT operations team to ensure that the information system and its physical infrastructure are destroyed in a way that protects corporate data and ensures that unauthorized users are unable to access sensitive information. Figure 2 illustrates how the CISO works with the business and technical leaders to establish cybersecurity deliverables and review gates that support the organization's security and risk posture (Death, 2017).

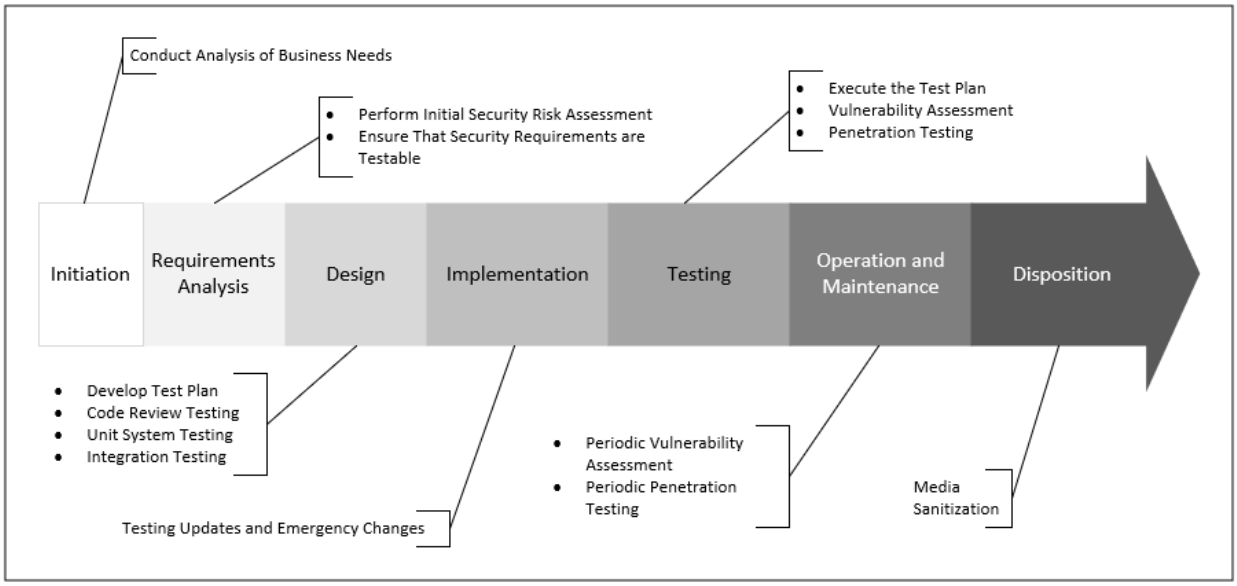

Figure 2. SDLC / SELC Phases (Death, 2017)

This integration level with the SDLC ensures a securely developed information system that will meet the desired project timelines through a fully integrated project planning process. Additionally, since security is pushed to the left as part of the project planning process, the cost to implement a secure solution is reduced compared to a similar project with security delivered at the end of the project.

The CISOs Role Related to Data Protection

For the CISO to adequately protect the organization's information, a thorough data categorization and classification processes must be implemented to ensure that security controls are implemented commensurate with the data's value that resides on an information system (Sosin, 2018). It is impossible to adequately protect an information asset without an adequate understanding of the data that resides on the system (Hulitt & Vaughn, 2010). Standards exist that allow the CISO to work with mission-level data owners and information technology custodians to determine the criticality of the information that is managed by the organization.

The National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 199 (NIST, 2004) provides the necessary guidance that allows the CISO to determine the information types that reside in an environment while also assessing the criticality of the information systems being used to host the data. Analysis from the information categorization is then used to determine how critical the data and information system is to the organization, which allows the technical team to assign information security controls to the IT systems that protect the technical implementation and data. The CISO plays a crucial role in establishing and maintaining an asset inventory that encompasses all technology and data assets in the organization. Asset management allows the organization to identify technology that must be managed by the organization's technical team. Once a complete asset inventory has been established, and a comprehensive data categorization has been completed, the CISO can establish security controls for the implemented and continuously managed environment.

The CISOs Role Related to Information Security and Risk Management

Information Technology security risks exist within organizations that could seriously affect a business's ability to operate its mission (Ogutu et al., 2018). To establish a resilient and enduring organization, risk management must be a consideration from a strategic perspective amongst organizational leadership (Steinbart, et al., 2018). To champion and develop an approach to enterprise information security risk management, the CISO must be engaged to ensure technical competence and integration of risk management capabilities (Karanja & Rosso, 2017). Without a practical approach to enterprise risk management, organizations cannot effectively identify, document, triage, and mitigate risks that may seriously affect the organization's ability to function (Ogutu et al., 2018). Enterprise risk management ensures that organizations can manage risks as identified (Kure, Islam, & Razzaque, 2018). Effective risk

management allows the organization to establish a management practice that considers the organizational risk appetite while allowing new threats to be mitigated, causing harm in a cost-effective manner (Webb, Ahmad, Maynard, & Shanks, 2016). The CISO is the critical information security leader for an organization (Karanja, 2017). As such, the CISO is responsible for establishing the culture where the information security program can grow and thrive. The enterprise information security risk management program is a critical component of an effective information security program (Kure et al., 2018).

Implementing adequate information security and risk management program capabilities within the organization are tied together as the risk management program builds on the operational and management controls present in the information security program (Death, 2017). As the top information security leader for the organization, the CISO will work with organizational executives to ensure that the information security program meets the needs and requirements of the mission of the organization (Hooper, & McKissack, 2016). In this way, the CISO is working to integrate the information security program into the organization's business and mission. Establishing an active integration of the information security program with the organization's mission leaders serves as an excellent opportunity to determine the organization's risk appetite. The risk appetite for an organization is where an organization allows a predefined level of risk to exist. Any amount of risk beyond the predefined level is the risk appetite of the organization. Any risks that exceed this level are mitigated and reduced to acceptable levels as defined by organizational leadership (Ogutu et al., 2018).

When discussing risk management, it is essential to understand where risk is owned within the organization. Ultimately, a risk to the organization is owned by the senior-most position within the organization. Depending on the organization, these senior-level positions may

be Board level or C-Suite positions (Murphy, 2018). While risk is owned by the most senior-level individuals of an organization, risk is managed by all levels within in an organization. (Ogutu et al., 2018). The managers and implementers of an organization take the risk appetite concepts developed with senior leadership support and develop an Enterprise Information Security Risk Management framework that effectively combines the risk appetite of senior leadership with actual technical considerations implemented by the enterprise (Dombora, 2016). This risk management approach allows a risk-based focus to information security decisions when conducting information system planning and implementation. Another essential part of risk planning that the CISO plays is data discovery and categorization (Karanja & Rosso, 2017).

In performing a proper risk assessment, organizational data assets must first be identified and assessed related to their organization's value. Not all information systems and data have the same value to the organization. The CISO helps the organization by leading an analysis of data assets that ensure that data is protected commensurate with its value (Ogutu et al., 2018). A proper assessment of data value is essential because data assets with a low value to the organization should not be protected like critical intellectual property. Conversely, critically important data should not be left unprotected (Death, 2017). By performing an effective data categorization, the CISO ensures that data assets are appropriately protected in line with organizational risk considerations.

The CISO works through the organization's business functions to ensure that risk management is integrated into the mission's strategy. From a business operations perspective, the CISO works with organizations like HR or Finance to ensure that their mission-critical data and information systems are protected commensurate with the value placed on them by the business units and executive leadership (Hooper & McKissack, 2016). The CISO will act as an

intermediary between the business units and information technology. In this way, the CISO can translate business requirements into technical security requirements that are implementable by the IT organization (Granneman, 2018). The CISO works with the IT Group of the organization directly to ensure that information security requirements are built into all enterprise information systems (Haqaf & Koyuncu, 2018). The CISO ensures that information security requirements are built into the System Development Lifecycle of an organization that results in more secure and less risky technology implementations (Death, 2017). The CISO also works with organizational personnel verifying that they are trained on their responsibilities related to information security (Cain et al., 2018). Practical training ensures that each user understands their role in establishing a resilient organization, protected from harm, and operating with minimal risk. The integration of all of these capabilities serves to develop a robust risk management practice led by the CISO to support a risk reduction plan that supports the goals and vision of the organization's executive leadership (Murphy, 2018).

Synthesis of Literature

The literature reviewed as part of this study included the available and recent scholarly literature related to the chief information security officer's role. Three themes presented themselves throughout the literature review. The three themes identified through the literature review are business integration and environmental understanding, information security strategy and design, effective communications, and organizational change management. There was a clear connection made throughout the literature related to the CISOs role and the importance of business integration and environmental understanding when developing and implementing an information security program for the enterprise (Alexander & Cummings, 2016). Cybersecurity should be viewed as a business enabler and should be strategically aligned with the business's

mission. The CISO must work to be an enabler of the mission to ensure that the information security program enables business objectives and adds value to mission capabilities (Rothrock et al., 2018). The CISO is critical to the success of the information security program and an organization's ability to be resilient (Murphy, 2018) and should be selected with care and the business's needs in mind (Granneman, 2018).

When focusing on environmental concerns, scholarly literature identified the areas of focus for the CISO around organizational culture and regulatory compliance. Organizational culture is the shared experiences a group of people has related to their company's nature and how they fit into the organizational structure (Schein, 2017). The CISO works to develop an information security culture where employees understand their role in protecting the organization from cybersecurity threats (Granneman, 2018). Both organizational and information security culture influence each other. The CISO is responsible for establishing the organization's information security culture and influencing organizational culture leading to positive security outcomes. (Tang et al., 2016). Penalties from regulators drive a greater need to implement cybersecurity protections (Doherty, Ashurst, & Peppard, 2012).

Information security strategy and design were highlighted across the literature and is a critical skill needed by the CISO to execute their duties (Steinbart, Raschke, Gal, & Dilla, 2018). The strategy's focus is not only associated with technology but also on operational and management competencies (Karanja, 2017). From an operational perspective, the CISO must understand how to effectively establish policies and procedures to effectively educate and govern the organization (Choi, 2016). Organizational risk tolerance must be considered when developing the information security program considering the organization's risk appetite when designing the information security program and safeguards for individual information systems

(Ogutu et al., 2018). From a management perspective, the CISO must ensure that effective processes and procedures are developed and promulgated across the organization for capabilities like configuration and change management (Cain et al., 2018). Configuration and change management plays a crucial role in ensuring effective cyber hygiene practices, ensuring that the organization is appropriately managed to defend itself against threat actors. From a technical perspective, the CISO implements tools and processes that ensure information systems are adequately secured and monitored. Vulnerability identification and mitigation techniques must be implemented to ensure a managed and effective security posture (Granneman, 2018). While the CISO implements technologies that ensure sufficient visibility for vulnerabilities and immediate response to threats (Karanja, 2017), capabilities must also be implemented that ensure information security safeguards are built into information systems (Kulkarni, 2018). Implementing information security capabilities as part of information system development helps ensure that the information system has adequate integrated security controls and that costs are better controlled related to security control implementation (Alexander & Cummings, 2016). Technical debt accrues on a technical project; the longer security requirements are not applied to the IT projects design process. Early in the project life cycle, security requirements must be introduced, and those requirements must be technically implemented through the design process. Once an information system has been designed, it can become very costly to retrofit, repair, or replace faulty design parameters (Granneman, 2018).

Effective communications and organizational change management were identified throughout the literature as a foundational aspect of information security program management and an essential skill needed by the CISO (Karanja & Rosso, 2017). CISOs have been identified as change agents within the organization and typically drive organizational-wide changes across

the organization at the enterprise level (Karanja & Rosso, 2017). Part of the CISOs role is communicating across the organization the roles and responsibilities for cybersecurity for every job function (Murphy, 2018). Everyone in the organization must understand the role they play from a cybersecurity perspective. All roles in the organization must receive training related to their cybersecurity responsibilities (Cain, Edwards, & Still, 2018). Specific roles and processes should receive special attention to ensure a resilient organization. From an executive perspective, cybersecurity is an active topic being discussed in boardrooms and with C-suite leadership (Rothrock et al., 2018). The key to being effective in this case is ensuring that the CISO provides the needed information to executive leadership. A risk-based decision can be made quickly, and action can be taken (Ogutu et al., 2018). Increased resilience should be a focus for organizations when discussing cybersecurity with the board (Cain et al., 2018). Company leadership should be educated on security issues so that appropriate risk-based decisions can be determined. A common taxonomy should be developed when communicating with organizational leadership to reduce confusion, allowing for quicker and more decisive executive decision making related to security risk (Rothrock et al., 2018). When focusing on organizational change, the CISO develops and communicates plans that drive organizational change and positive security outcomes through training and awareness of security roles and responsibilities. Once individuals understand their responsibilities, security is built into new information systems and processed across the organization. The processes here are not focused merely on technologies. As part of organizational change and a healthy information security culture (Tang et al., 2016), business processes are adapted to ensure that company critical information is handled safely and in accordance with the organization's risk appetite (Granneman, 2018).

Conclusion

The three themes identified through the literature review are business integration and environmental understanding, information security strategy and design, and effective communications and organizational change management. The role of the CISO is not well understood, and a great deal of difference exists between organizations regarding how the role is implemented (Karanja & Rosso, 2017). Recently identified security breaches highlight the need for more CISOs across industry verticals (Hooper & McKissack, 2016). CISOs have been identified as change agents within the organization and typically drive organizational-wide changes across the corporation at the enterprise level (Murphy, 2018). Influential and inspirational leadership directly affects the adoption and support of an organization's information security program (Choi, 2016). As a leader, the CISO plays an essential role in shaping an information system's sustainability beyond just the technical implementation to include an information system's operational and management responsibilities. Information technology plays an ever-increasing role in mission performance due to the value that information technology brings to mission delivery (Mithas & Rust, 2016). As a result, IT investments and the security controls protecting that investment should be aligned with the business's mission. The CISO works with the technical teams to establish requirements and goals that drive positive information security results across organizational information systems (Granneman, 2018). Effective information security governance and top management support are critical to achieving these positive information security outcomes (Rothrock, Kaplan, & Oord, 2018).

Cybersecurity should be viewed as a business enabler and strategically aligned with the business (Granneman, 2018). The CISO is critical to the information security program's success and should be selected with care and the business's needs in mind (Hooper & McKissack, 2016).

Penalties from regulators drive a greater demand in the industry to implement cybersecurity protections making the role of the CISO even more critical (DOD, 2019). Cybersecurity is an active topic discussed in boardrooms across the country (Rothrock, Kaplan, & Oord, 2018). The key to being effective from a board and information security perspective is asking the right questions. Increased resilience should be a focus for organizations when discussing cybersecurity with the board (Cain et al., 2018). Company leadership should be educated on security issues to determine appropriate risk-based decisions (Ogutu, Bennett, & Olawoyin, 2018). When discussing cybersecurity with the board, the CISO must differentiate between security (antivirus) and resiliency (business uptime). Cybersecurity and resilience should be a company's board's strategic business goal (Rothrock et al., 2018). Organizational culture is the shared experiences a group of people has related to the company's nature and how they fit into it (Schein, 2017). Information Security culture is how employees view their role in protecting the organization from cybersecurity threats (Tang et al., 2016). Both organizational and information security culture influence each other (Nasir, Arshah, Hamid, & Fahmy, 2019). The CISO is responsible for establishing the organization's information security culture and influencing organizational culture leading to positive security outcomes (Santos-Olmo et al., 2016). The CISO plays an essential role in establishing information security culture by ensuring that cybersecurity roles and responsibilities are promulgated effectively across the organization so that everyone in the organization understands the role they play from a cybersecurity perspective (Murphy, 2018).

While popular and trade articles have provided significant commentary on the CISO role, little academic research has been conducted (Karanja & Rosso, 2017). Additionally, after reviewing the limited academic research available on the role of the CISO, no academic research could be identified about the role of the CISO for a government contracting organization. This

avenue of research provides an excellent opportunity to offer a meaningful study to further the overall body of knowledge related to information technology, management, and cybersecurity as little academic research exists on the subject of the CISO and no research exists for CISO within government contracting organizations. Consensus does not exist related to the roles of the CISO in the government contracting organization in support of meeting U.S. federal government requirements related to cybersecurity. Therefore, this qualitative classical Delphi study identified the roles of the CISO in a government contracting organization as viewed by a nationwide panel of security experts. Chapter Three provides the details related to the methodology utilized to execute this research study.

CHAPTER 3. METHODOLOGY

Introduction

The purpose of this qualitative classical Delphi research study is to identify the role of the CISO in a government contracting organization utilizing a panel of security experts and to determine the extent to which there is a consensus of opinion among these experts related to the importance of these roles. The general problem under investigation in this study is that government contracting organizations face the threat of not establishing new or maintain existing contractual work due to non-compliance with U.S. federal cybersecurity requirements. The specific problem is that executives within government contracting organizations do not understand how to strategically align the CISO within the company to support an enterprise digital strategy that includes U.S. federal cybersecurity requirements. This study offers an excellent opportunity to further the body of knowledge related to information technology and information security to better integrate the key cybersecurity leadership role within the government contracting organization. This study's business/mission application is to allow government contracting leaders to better plan for, understand, and utilize the CISO role. Contractors will be able to better use the CISO as both a strategic and tactical leader to establish long-term plans and short-term protections that will result in a more resilient organization and information technology infrastructure.

A study related to the role of the CISO in the U.S. federal government contracting organization is very timely, considering the increasing focus of the U.S. federal government on supplier cybersecurity practices (DOD, 2019). While there is limited academic research on the role of the CISO (Karanja & Rosso, 2017), no research could be found on the role of CISOs in government contracting organizations. The ever-growing pace of digital transformation in our

nation (Andriole, 2017) brings into focus the need for information security and a clear understanding of the role of the CISO for the government contractor. Consensus does not exist related to the role of the CISO in the government contracting organization in support of meeting U.S. federal government requirements related to cybersecurity. This study answered the following research questions. What are the roles of the CISO in a government contracting organization for establishing and maintaining an organization's information and data security as viewed by a panel of security experts? To what extent is there consensus among a panel of security experts as to the roles of the CISO for establishing and maintaining a government contracting organization's information and data security?

Design and Methodology

A qualitative methodology was selected for this study as little academic research exists on the subject of the CISO and no research exists for CISO within government contracting organizations (Karanja & Rosso, 2017). This study was exploratory in nature since little has been written academically about the CISO. The study utilized questionnaires and expert interviews to gather data and develop an understanding of the role of the CISO within a government contracting organization. A qualitative exploratory methodology is the best approach to gathering data in support of this study since little academic work exists on the topic. The researcher collected the opinions from practitioners to develop an understanding of the role of the CISO within a government contracting organization.

Quantitative research is best suited for mathematical analysis. This study analyzed the individual opinions and experiences of a panel of experts. Quantitative research is not suited to gathering the concepts and experiences of study participants, as this method is designed to understand how the relationship between variables influence a business problem (Creswell &

Creswell, 2018). For this reason, a quantitative approach is not appropriate for this study. This study aims to understand what experts consider vital as it relates to the role of the CISO in a government contracting organization. A Delphi study results in the researcher getting consensus among experts (Creswell & Creswell, 2018). Additionally, considering the executive roles that CISO's fill within their organizations, direct interaction to conduct interviews would be challenging to execute due to their time constraints. Therefore, Delphi is the best methodological fit for this study. Thus, this study employed a qualitative Delphi methodology which examined the experiences and perception of an expert panel of cybersecurity experts in the United States to determine where consensus exists regarding the roles of the CISO within a U.S. federal government contracting organization (Whitten, 2008).

The RAND Corporation originally established the Delphi method in the 1950s. The technique was designed to rapidly develop consensus amongst a group of military experts supporting the United States national cold war planning effort (RAND Corporation, 2016). The Delphi method employs multiple rounds of interviews, allowing a researcher to analyze the interview responses of a panel of experts leading to a refined understanding of a given business problem (Hsu & Sandford, 2007). A qualitative methodological approach has been selected for this study due to the limited scholarly information related to the role of the CISO. Qualitative research is used where little information is available on the area being studied (Creswell & Creswell, 2018). As limited information exists on the role of the chief information security officer for a government contracting organization, a qualitative approach provides the tools needed to interact directly with industry experts allowing the researcher to gain new insights on the role (Yin, 2016).

As the CISO role is a relatively new addition to the C-Suite, there is limited academic research on the role of the CISO (Karanja & Rosso, 2017). Additionally, no identified research could be found on the role of CISOs in government contracting organizations. While there is limited research available on the subject, the role is being increasingly adopted across industries with many opportunities to build a highly qualified panel of experts that can assist in developing a better understanding of the skills, roles, and responsibilities of the CISO (Hooper & McKissack, 2016). In this case, the Delphi method provides an excellent opportunity to examine the role of the CISO as it can be used to develop consensus (Hsu & Sandford, 2007), where a lack of clear consensus exists across scholarly and practitioner literature (Karanja & Rosso, 2017).

Participants

Based on statistics reported, on January 4, 2019, the total number of individuals employed in a cybersecurity career totaled 716,000 (Crumpler & Lewis, 2019). A review of the same statistics reported on January 8, 2020, revealed that the number of employed cybersecurity professionals has risen to 997,058 with a total cybersecurity job opening vacancy of 505,316. Of those job openings, 65,234 positions are categorized as leadership positions (Cyber Seek, 2020). These unfilled cybersecurity leadership positions, in addition to filled positions, are of critical importance to organizations as they set the direction for risk management and ensure that cybersecurity strategy is aligned with the mission of the organization (Choi, 2016).

This study's population consists of cybersecurity experts who currently hold or have held a position of leadership related to the field of cybersecurity within an organization that supports the U.S. federal government in a contracting capacity. Cybersecurity leaders across industry verticals, including those in government contracting organizations, experience many of the same

challenges related to protecting their organizations from new threats and adversaries. However, the federal government's unique requirements on its contracting community related to cybersecurity standards result in greater scrutiny from top-level organizational executives. This increased focus occurs because poor cybersecurity performance can lead to reduced competitiveness resulting in an inability to maintain current and win future contracts. For this reason, cybersecurity leadership from government contracting organizations was selected as they are best positioned to understand the business problem under investigation as part of this study.

This study's sample comprised cybersecurity professionals with at least 15 years of experience in the technology field and has held a leadership position within a government contracting organization’s cybersecurity or information security division. While establishing the panel of experts for this study, care was taken to ensure that participants can speak on the role of the CISO versus how a specific organization implemented the role. Additionally, the researcher sought out a larger initial pool of potential expert panelists using professional organizations aligned with the government contracting community. Potential panelists were reviewed based on their organization affiliation, job description, role related to cybersecurity leadership, and their understanding of U.S. federal government contractor security requirements. Expert panelists who met the study's criteria were contacted via email or LinkedIn to establish interest in the study. Once initial interest had been established, a formal letter was sent electronically to the participant that thoroughly explained the study allowing for informed consent (Cooper & Schindler, 2014).

Little consensus exists for the number of expert panelists that should be part of a Delphi study. However, a review of academic literature on the Delphi methodology suggests that a Delphi panel should be between seven and 12 participants (RAND Corporation, 2016). This

study exceeded the Delphi panel member recommendation with a total of 19 expert panel members. The criteria used to select experts for this Delphi study are described below.

- Each member of the panel must have at least 15 years' experience in the technology field.
    - Five of those years serving in the information technology field must have been directly focused on cybersecurity or information security leadership, focusing on developing, implementing, and managing the day to day and strategic aspects of a security program for a government contracting organization.
- Position titles appropriate for information or cybersecurity professionals include chief information security officer, Chief Security Officer, and Information Security Manager.
    - As there is little consensus related to the title of an information or cybersecurity leader (Karanja, 2017), other position designations were reviewed as potentially acceptable for inclusion into the expert panel selection criteria.
- Each member of the expert panel must have direct experience managing regulations and standards related to securing government contractor enterprise information systems in accordance with U.S. federal government cybersecurity standards.
    - One or more of the following standards must be part of the expert panelists experience to qualify for the study:
        - The National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171 standard "Protecting controlled unclassified information in nonfederal systems and organizations" (Ross et al., 2018).
        - The Department of Defense Cybersecurity Maturity Model Certification (DOD, 2019).

- The Defense Federal Acquisition Regulation (DFAR) Supplement 252.204-7012 (Sweeney, 2018).
- The International Organization for Standardization ISO27001 information security standard (ISO, 2019).

The cybersecurity standards utilized by the U.S. federal government have been developed mainly to ensure that the government's sensitive information being stored on contractor information systems is protected from misuse and fraud. As such, a competent expert panel consisted of members that have experience implementing governmental cybersecurity standards for their company and have experience with the organizational change that resulted as part of the implementation. This experience is critical to understanding the CISO and how this leader works within an organization to bring about positive change for the organization related to cybersecurity, compliance, and resilience.

The information and cybersecurity fields are still considered young from a professional standpoint, and professional cybersecurity degrees are a relatively new phenomenon. Standards for Cybersecurity education are new and have only been developing over the past decade (Parrish et al., 2018). Cybersecurity education is a new area of education primarily due to the relatively short period of time that the discipline of cybersecurity has existed versus other computer-related fields like computer science or information technology (Howles, Romanowski, Mishra, & Raj, 2011). As a result, imposing specific cybersecurity requirements from an educational perspective on study participants could lead to security leaders not being selected. They may have completed their academic journey before cybersecurity degrees became available from universities. For this reason, a specific degree type was not be required to participate in the study.

Implementing the Delphi methodology for this study allowed the researcher to gather data from a diverse panel of experts with varied educational backgrounds that all supported the implementation of security programs within a government contracting organization. Based on the lack of consensus related to the CISO role (Karanja, 2017), it was decided to cap the expert panel members' qualifications to those defined above. Restricting the panel's qualifications any further could lead to individuals being eliminated from the study that are experts in the field but unable to meet unnecessary researcher defined requirements.

As part of this study's selection process, the researcher analyzed the following information related to potential panelist qualifications before candidates being admitted into the study: Title; Job duties; and experience implementing a security program with a focus on security standards implemented. Based on a careful analysis of panelist's qualifications, the researcher selected study participants leading to a properly constructed panel of industry experts supporting this study’s data-gathering requirements.

Setting

To establish the study’s panel of experts, the researcher utilized LinkedIn to recruit potential members for the expert panel. Potential panelists were invited to join the study based on their job title and recent employment. The researcher contacted potential panelists based on whether they worked for a government contracting organization and if they hold the title of chief information security officer, Chief Security Officer, Information Security Manager, or another role that has similar responsibility. Based on a positive review of the contacted potential panelists: title, job duties, experience implementing a security program, and government cybersecurity standards implemented, the panelists were admitted into the study.

The Microsoft 2019 annual report defines LinkedIn as a social network designed to connect professionals around the world, assisting them in becoming more successful and productive (Nadella, 2019). LinkedIn is the largest professional network on the Internet, with more than 645 million members creating an opportunity to quickly and easily reach out to potential panelists. LinkedIn profile pages include the individual's name, necessary information related to an individual's career, and contact information. This information can be utilized to validate the study's expert requirements, which is required to ensure a successful panel under the Delphi method. LinkedIn is a satisfactory setting to recruit experts for use in this study. It has been identified that LinkedIn profiles are updated regularly, leading to information that can be used to narrow down potential panel participants and validate panel participation qualifications (Lops, De Gemmis, Semeraro, Narducci, & Musto, 2011). Based on the electronic availability of participant job information and the ability to quickly contact potential participants, the LinkedIn platform provides a logical choice to identify and communicate with the experts that supported this study.

The researcher for this study utilized an iterative series of questionnaires that consisted of three rounds of interviews being delivered electronically via SurveyMonkey . Round 1 of this study was an open-ended electronic questionnaire used to establish consensus amongst a group of experts related to the management reporting relationship and fundamental roles that must be possessed by a CISO for a government contracting organization. The Round 2 questionnaire asked the panel of experts to rank the identified reporting relationships and roles needed by a government contracting CISO related to their importance for an organization. As part of this round, the expert panel was additionally asked to provide a narrative for each role. Asking for this information helped to construct a standard definition for the roles that were under

investigation. The expert panel received a summarized response from Round 1 to allow for consensus-building during Round 2. The Round 3 questionnaire utilized the results from Round 2, where consensus was achieved to provide the expert panel with an opportunity to introduce new data and affirm their agreement with the data collected in rounds one and two. The researcher worked with all study participants over the phone, email, and LinkedIn to answer any questions and alleviate any technical impediments related to answering survey questions. The purpose of direct participant communication was to ensure a mechanism to troubleshoot issues related to study participation. This study aimed to carry out all survey-related activities in an electronic self-service format utilizing the SurveyMonkey tool.

Analysis of Research Questions

The Delphi methodological choice provides a framework by which the researcher establishes an expert panel of subject matter experts to understand the panel members' perceptions and experiences. This study's research question is well suited to be implemented as part of a Delphi research method. The survey questions used in this study were delivered through electronic interviews that consisted of multiple rounds of questionnaires (Hsu & Sandford, 2007). The researcher for this study utilized an iterative series of questionnaires that consisted of rounds of interviews being delivered electronically via SurveyMonkey. Round 1 of this study can be found in Appendix B. Round 1 was developed using the study's conceptual framework, currently available scholarly data, and the most recent practitioner analysis on the role of the CISO. Round 1 was presented to the study participants as an open-ended electronic questionnaire. The literature review performed as part of chapter two of this study reviewed these concepts and served as the knowledge foundation for the questionnaire used in this study.

The concepts being explored in Round 1 begin with developing the roles that a chief information security officer in a government contracting organization should possess, through the lens of the ever-increasing cybersecurity requirements being levied by the U.S. federal government (Ross et al., 2018; Sweeney, 2018). It is accepted that information technology plays an ever-increasing role in the government contractor's mission performance due to the value that IT brings to mission delivery and contract execution success. As the role of information technology has changed, so has the role of information security leaders within the government contracting organization (Karimi-Alaghehband & Rivard, 2014; Mithas & Rust, 2016).

The questions associated with the Round 1 questionnaire support answering the research question developed in chapter one. The Round 1 questionnaire retrieved the observations and experiences of experts in the cybersecurity field to understand the determine a baseline of chief information security officer roles. The expert panel was asked to rank specific CISO roles and provide a brief explanation of the role. This information served to inform the study of the importance of roles needed to lead a government contracting organization to support a resilient, secure, and compliant organization that meets the U.S. federal government's cybersecurity requirements. The conceptual foundation of the study serves as a basis for the study and the Round 1 questionnaire. The conceptual framework for the study is Organizational Culture Theory. Understanding how the role of the CISO integrates with the mission of the organization and serves to support and change the organizational culture of a government contracting organization was crucial to understanding how the roles needed by the CISO support the requirements for a business. The Round 1 questionnaire served to identify themes and patterns based on the assembled expert panel's experiences and viewpoints.

Once the themes and patterns related to the role of the CISO were identified, these were used to support the Round 2 questions that are presented in Appendix C. This round was used to determine consensus related to the importance of CISO roles being integrated into the mission of a government contracting organization. Round 1 results were analyzed for inclusion in the Round 2 questionnaire. The Round 1 questionnaire was associated with ranking and defining the critical roles needed by a government contracting organization's CISO. The Round 2 questionnaire sought to gain consensus from the panel of experts related to their role rankings and definitions for a government contracting CISO. As part of Round 2, the expert panel was asked to provide a rationale for their ranking selection for each role rankings. Finally, the Round 3 questionnaire located in Appendix D provided the expert panel with an opportunity to introduce new data and affirm their agreement with the data collected in rounds one and two of the study.

This information informed the researcher of each role's importance for the government contracting CISO as perceived by the expert panel. The data was analyzed to look for themes that can provide further insights into how the roles of the CISO support the government contracting organization's mission success. Factors were cited by the expert panel that allowed the researcher to draw conclusions related to the roles required and their importance for a CISO to be successful within a government contracting organization.

Role of the Researcher

My role in this study is to serve as an instrument to carry out the processes and procedures related to study execution. Utilizing electronic mechanisms, I managed the expert panel and the three rounds of Delphi surveys to develop consensus amongst the panel. I also collected and analyzed the data associated with the questionnaires to develop conclusions and understand the data trends until saturation was attained. I have over 20 years' experience

implementing enterprise Information Technology solutions across government and government contracting organizations. I served within the U.S. federal government for over eight years as a cybersecurity professional and a Contracting Officer Technical Representative (COTR). In this role, I implemented extensive cybersecurity controls and was responsible for ensuring that suppliers met agency cybersecurity requirements. Additionally, I have over five years of experience serving as a chief information security officer for a government contracting organization. My experience provides a unique skill set where both sides of the acquisition process from a public and private sector perspective have been carried out. I have been responsible for establishing supplier cybersecurity requirements as a government employee and establishing an information security program designed to meet the U.S. federal government cybersecurity requirements as a CISO for a government contracting organization. These skills provide me with the knowledge, skills, and abilities necessary to carry out this study's analysis requirements.

Credibility and Dependability

This study's credibility brings to the Information Technology body of knowledge is defined by the quality and integrity of the research design related to its planning and overall implementation. Once data was collected from study participants, a complete and thorough analysis of the data to develop conclusions that support government contracting organization decision-makers was performed and serves to define the success of this research study (Creswell & Creswell, 2018). This study’s success is further defined by providing executives within government contracting organizations the information to strategically align the CISO to support an enterprise digital strategy that includes U.S. federal cybersecurity requirements (Ross et al., 2018; Sweeney, 2018). Without this information and a strategy to implement cybersecurity

leadership, a government contracting organization may not be able to establish new or maintain existing contractual work as a result of non-compliance with government requirements (Freedberg, 2019). As such, this research contributes to both the body of knowledge in the Information Technology and Information Security field and serves practitioners and organizational executives by adequately aligning the CISO role with their organizations' missions to support organizational resilience and compliance with U.S. federal government cybersecurity requirements.

Utilizing a qualitative Delphi methodology to identify the roles required of a CISO in a government contracting organization is appropriate. It uses the input of a panel of experts from the cybersecurity industry to rank and define the roles needed to be successful as a CISO in these organizations. The methodological choice of using Delphi for this study means special care was taken when developing the expert panel that participated in the study. Establishing participants' qualifications is critical as the expert panel was the primary input to support this study's data gathering activities. Therefore, the researcher analyzed each panelist’s qualifications to ensure that they meet the requirements as defined above to be invited to participate in this study.

Another critical aspect of establishing a well-functioning panel is the establishment of well-defined privacy and anonymity protocols. These protocols serve two essential functions that are critical to the success of the study. First, the protocols help ensure that an expert cannot be positively identified as a study participant. Protecting identity helps to ensure that the participant does not receive any type of reprisal for their participation in the study due to any answers that they may provide. This protocol also helps to ensure that any sensitive information provided by a participant cannot be tracked back to the individual, providing the information that could be traced back to a specific organization. This study is concerned with expert opinion and not the

particular implementations being performed by an individual company. This anonymization protocol helps protect the participant and any organizations that the participant may have worked for in the past. The anonymization and privacy protocols also help to remove any collusive behavior amongst the expert panelists. Part of conducting a successful Delphi study is ensuring that all the panelists provide their unbiased perceptions and observations unassociated from the opinions of the other panelists. Ensuring that each panelist is unaware of the others' participation in the study serves to ensure that each member in the study provides their point of view in an unbiased and independent manner (RAND Corporation, 2016). Based on the analysis of expert qualification and the establishment of appropriate privacy and anonymity protocols, the researcher ensured the successful recruitment of experts who provided independent expert opinions for this study.

Data Collection

The researcher compiled data from the assembled panel of cybersecurity experts utilizing the Delphi methodology and employing multiple rounds of questionnaires to elicit participant observations and perspectives related to the chief information security officer's role within a government contracting organization. The questionnaires were delivered electronically, utilizing the SurveyMonkey tool. The researcher collected and analyzed the data associated with the questionnaires to develop conclusions and understand the data trends until saturation was attained. The Round 1 questionnaire was designed with open-ended questions that elicit feedback from experts to better understand the CISO in the government contracting organization. The Round 1 questionnaire additionally gathered the rationale behind the panel member’s ranking of a specific role. After the Round 1 questionnaire was completed successfully, the researcher analyzed the results to understand better the themes emerging from the panel responses. Based

on the answers to the Round 1 questionnaire, the researcher developed the Round 2 questionnaire. The questionnaire in Appendix B was field-tested to set expectations for the actual study and ensured that the processes, procedures, and survey instrument operated as expected. This process served to increase the likelihood of survey success and the successful collection of accurate data (Bryman, 2012).

The Round 2 questionnaire asked the expert panel to review the data captured from the Round 1 survey related to the roles of the CISO and the CISO's management reporting relationship. The purpose of this review was to gain consensus from the expert panel about the information presented in Round 2. The information presented in Round 2 consisted of the ranked CISO roles, synthesized role definitions, and the optimal management reporting relationships for the CISO. All information given to the panelists was accompanied by an option for a narrative to allow the panelist to justify their survey question decisions. This information allowed the researcher to analyze the panel's responses to determine a deeper meaning behind the responses. This information will help business leaders develop plans and strategies that properly incorporate the CISO and an information security program that supports U.S. federal government cybersecurity requirements within their company. Finally, the Round 3 questionnaire provided the expert panel with the opportunity to introduce new data and affirm their previous responses. In this way, final consensus can be reached amongst panel members.

Member checking was used as part of this study's data collection methodology to improve the research's validity, accuracy, and credibility. (Birt, Scott, Cavers, Campbell, & Walter, 2016). The study participants were contacted to conduct member checking during Round 1, two, and three of this Delphi study. As part of member checking, the participants provided feedback, additional supplemental details, and verification of information supplied as part of

each survey round. The participants were allowed to supplement, modify, delete, and confirm their responses during each round of the Delphi study. Member checking enhances the overall trustworthiness of the data collected as part of qualitative research (Candela, 2019). The member checking technique used during this study allowed the researcher to ensure that the data associated with the roles of the CISO, the definitions of those roles, and the reporting structure required for a CISO adequately portrayed the expert panel's views. By implementing member checking, each participant in the study provided feedback that allowed the researcher to ensure that each round's final results included the participant's experiences and perceptions.

Data Analysis

As the methodology being used for this study is the Delphi method, the researcher's primary goal was to analyze the expert panel's responses to determine consensus. As a result, the researcher examined responses to the Round 1, two, and three questionnaires to assess where themes and patterns emerged from the expert provided responses (Hsu & Sandford, 2007). Based on an analysis of the themes and patterns related to survey data, the panel's narrative responses, and available literature, the researcher was able to understand the emerging themes related to the roles required for the CISO within a government contracting organization. The researcher's role in this study was to serve as an instrument to carry out the processes and procedures related to study execution. All study participants received the same number of questionnaire rounds and questions, ensuring uniformity and consistent data gathering. The researcher collected and analyzed the data associated with the questionnaires to develop conclusions and understand the data trends until saturation was attained.

NVIVO and Microsoft Excel software were employed to interpret data collected from the multiple rounds of expert surveys. Utilizing these tools allowed the researcher to perform

inductive and deductive analysis for study participant responses. This analysis allowed the researcher to group the expert provided data into the patterns and themes present across the participant responses as a whole (Creswell & Creswell, 2018). Once the patterns and themes were identified as they relate to the role of the CISO for a government contracting organization, they were used to support additional rounds of questions during the data gathering phase and ultimately reinforced the data analysis phase of the study in Chapter 4 (Ghauri & Gronhaug, 2010).

Ethical Considerations

The study followed the procedures outlined by Capella University related to ethical standards in accordance with the Institutional Review Board (IRB) of the University. Based on different requirements across industries related to cybersecurity compliance and resilience, expert panelists were only selected with experience with government contracting cybersecurity requirements. The difference in both U.S. federal government requirements imposed on contractors and the contracting community's business practices can place precise requirements on the CISO. As a result, intermingling other business sectors within the study could result in inconsistent results that would not serve the government contracting community.

The researcher in this study has significant cybersecurity experience and experience related to implementing and managing information security programs as a CISO for a government contracting organization. As such, the researcher can potentially introduce bias into the study based on their experience. To limit the potential influence bias may have on this study, the researcher has implemented steps to ensure that selected panelists have not ever worked with the panelists or for the same company at any time. In this way, the researcher and panelist's perceptions and experiences were different and not based on an organization's common cultures.

The study did not initiate any formal interaction with participants until IRB approval had been received. As part of this study's execution, all study participants were provided with detailed research and personal privacy information. This information allowed study participants to make an informed decision about their participation in the study (Creswell & Creswell, 2018). Once participants received study-related information, all participants were required to agree to the informed consent agreement. The agreement template provided by Capella University was used in accordance with Capella IRB standards.

All participant information was anonymized to ensure personal privacy and ensure non-attribution related to participant responses. Due to the sensitive nature of the data being collected as part of this study, personal attribution could lead to an adverse effect on a participant's professional or social standing (Cooper & Schindler, 2014). Study data was managed securely, ensuring the participant's personal protections (Creswell & Creswell, 2018). All study data is maintained on an encrypted USB drive that meets government standards for encryption of data at rest (NIST, 2001). A data backup of all study data is maintained on a paid Microsoft Office 365 account. The Office 365 account is password protected and utilizes multi-factor authentication. The Office 365 account data is encrypted, utilizing the same standard used to encrypt the data repository located on the USB drive.

Conclusion

Chapter three provided a detailed explanation of the methodological approach for this study. This study employed a qualitative Delphi methodology which examined the experiences and perceptions of an expert panel of cybersecurity experts in the United States to determine where consensus existed regarding what makes the roles of the CISO within a U.S. federal government contracting organization (Whitten, 2008). The study utilized the expertise of 19

cybersecurity professionals that have at least 15 years of experience in the technology field and have held a leadership position within a government contracting organization's cybersecurity or information security division. The study was conducted primarily in electronic form utilizing LinkedIn, email, phone, and SurveyMonkey to accomplish participant interaction and data gathering. The researcher compiled data from the assembled panel of cybersecurity experts using the Delphi methodology and employed multiple rounds of questionnaires to elicit participant observations and perspectives related to the chief information security officer's role within a government contracting organization.

Once data was collected, a complete and thorough analysis of the data was conducted to support a government contracting organization's leadership related to effective business and mission integration of the CISO role into the organization. As the methodology used for this study is the Delphi method, the researcher's primary goal was to analyze the expert panel responses to determine consensus. As a result, the researcher examined responses to Round 1, two, and three questionnaires to assess where agreement existed and identify where themes were present in the panelist's responses. Themes were identified in the narrative responses that were integrated into the survey questions and were used to justify the expert panel's decisions. These narrative responses help illuminate the decisions related to role inclusion and the panel's subsequent rankings of the roles. Finally, the study followed a set of ethical considerations that served to ensure a reliable and consistent study that protected participants' rights. Chapter four presents the findings collected during the execution phase of the study. The findings discussed in chapter four include any identified themes based on the consensus of the expert panel discussing the role of the CISO within a government contracting organization.

CHAPTER 4. RESULTS

Introduction

The general problem addressed by this study is that government contracting organizations face the threat of not being able to establish new or maintain existing contractual work as a result of non-compliance with U.S. federal cybersecurity requirements. The specific problem is that executives within government contracting organizations do not understand how to strategically align the CISO within the company to support an enterprise digital strategy that includes U.S. federal cybersecurity requirements. The U.S. federal government is making great strides related to integrating cybersecurity requirements into solicitations for government contractors. The government is also developing standards that support the management of contractor cybersecurity certifications (Doubleday, 2019). The government has also developed research that supports the dire need for cybersecurity to be addressed as a whole of society concern, which includes government suppliers (Cyberspace Solarium Commission, 2020).

The purpose of this qualitative classical Delphi study is to identify the role of the CISO in a government contracting organization as viewed by a nationwide panel of security experts and to determine the extent to which there is a consensus among these experts as to the importance of the role. The research question for this study is presented below.

> RQ: To what extent is there a consensus among a panel of security experts as to the roles of the CISO as it relates to establishing and maintaining a government contracting organization's information and data security?

While conducting the research associated with this study that sought to understand better the role of the CISO within government contracting organizations, the researcher utilized a mixture of online and phone-based interviews. The study consisted of an expert panel that

comprised 19 technology executives that hold leadership positions within government contracting organizations. They are responsible for ensuring the implementation of U.S. federal government cybersecurity requirements. The data collected during this study was gathered through three iterative rounds that sought to gain consensus amongst the expert panel related to the role of the CISO. During this study, the collected data was reviewed against available literature to understand if this information provided a new understanding of the topic under investigation or if the data provides further support for already existing research that can now be applied within the U.S. federal government contracting community.

This study's outcome is an understanding of the roles that need to be supported by the CISO within a government contracting organization and definitions that can be used to understand the CISO role better. Another outcome of this study is understanding how the CISO should be positioned within the organization to be most impactful working to drive organization culture and change as it pertains to improving an organization's security posture.

Data Collection Results

Description of the Sample

The study utilized LinkedIn as the sole recruitment tool for the study. In addition to the researcher's LinkedIn feed, three groups were used on LinkedIn to recruit participants that met the study's inclusion criteria. LinkedIn group owners were approached before beginning the study, and site permission was secured from each group to begin recruitment activities.

The study's inclusion criteria included individuals with at least 15 years' experience in the technology field. Five years in the technology field must have been directly focused on cybersecurity or information security leadership. The focus area for cybersecurity must be on developing, implementing, and managing the day to day and strategic aspects of a security

program for a government contracting organization. Each expert panel member has direct experience managing regulations and standards related to securing government contractor enterprise information systems. This experience was aligned with U.S. federal government cybersecurity standards. The sample size for the study at the beginning of the study was 19. The researcher was responsible for utilizing LinkedIn, as mentioned above, to conduct all recruitments activities. The researcher developed a recruitment flyer that was posted to each LinkedIn group and the researcher's LinkedIn feed to recruit participants for the study. Potential participants contacted the researcher utilizing the researcher's academic email address and the LinkedIn private messages function, which were both provided to potential participants as part of the recruitment materials.

Once potential participants were identified, the researcher provided each respondent with a copy of the approved informed consent form, which had been approved by the Capella Institutional Review Board. Once respondents agreed to be part of the study, were deemed to meet the inclusion criteria, which was part of the informed consent, and accepted the informed consent, the Round 1 survey was provided. The Round 1 survey included the study's screening questions to ensure that all study participants met the research's inclusion criteria and that this inclusion information was adequately documented. The screening questions are located in Appendix A. The 19 individuals who participated in the study have immediate responsibility for ensuring that cybersecurity requirements are implemented within their organizations and are responsible for delivering cybersecurity capabilities that allow their organizations to meet the U.S. federal government contracting cybersecurity requirements. In Round 2 of the study, all 19 participants returned to complete the survey. Round 3 showed a slight drop in participation, with 17 participants taking part in the survey. A potential reason for participant drop off in Round 3

could be attributed to panel member scheduling conflicts and priorities (Keeney, Hasson, & McKenna, 2006). Even with the slight drop off in Round 3, a high participation rate was observed for the study. A potential reason for the high participation rate for this study is connected to the increase in cybersecurity requirements levied by the U.S. federal government and the need for government contractors to understand how to utilize the CISO position leading to better compliance with those requirements (DOD, 2019).

The study did not store personally identifiable information related to any participants as this information was not relevant to the study's completion. The researcher provided a reminder via email after six days of Round 1 being released. The reminder email was sent to remind the participants to open and complete the survey. Once Round 2 was released, the participants were provided a reminder to complete the study after four days. Finally, with Round 3, the study's participants were provided a reminder to complete the study after four days. There is no firm agreement on the proper sample size for a Delphi study, and the sample size is, in most cases, specific to the needs of the researcher or the particular situation that the study is being conducted in (Akins, Tolson, & Cole, 2005). An expert panel between 15 and 60 are recommended for Delphi Study's (Hasson, Keeney, & McKenna, 2000). Therefore there is sufficient expert participation as this study recruited and retained 19 for the first two rounds and 17 for the last round.

Data Analysis and Results

The data collected in the Round 1 survey consisted of open-ended questions and a predefined listing of roles. The selected roles are acknowledged in the literature as being essential to the success of the CISO. The data analysis involved conducting a thorough examination of the participant's responses. These responses were synthesized into a single

narrative that could be delivered to the expert panel in subsequent rounds to gain consensus related to both the roles critical to the success of the government contracting CISO and the definition of those roles allowing for a consistent understanding of what those roles mean. The study also collected free form responses from the participants. These responses were used to provide further insight as it relates to the various roles of the CISO, the placement of the CISO within the organization, and what needs to be in place for the CISO to be successful related to implementing U.S. federal government cybersecurity requirements.

This section organizes the study's data collection results into the three rounds that were used to accomplish the Delphi study. The NVivo application was utilized to categorize participant responses in alignment with Organizational Culture Theory. The study data used for analysis was directly imported from SurveyMonkey into NVivo. For each of the open-ended questions throughout the three rounds, themes were identified and coded, creating themes that were aligned to Organizational Culture Theory. For closed-ended questions, data was imported directly to Microsoft Excel from SurveyMonkey for analysis. The following sections describe the data analysis associated with each question, the themes that arose from participant responses, and the results of questions designed to reach consensus related to the role of the CISO within a government contracting organization.

Data Analysis Round 1

The first round of this Delphi study took place between July 21, 2020, and August 08, 2020, where the researcher collected responses from 19 Technology experts who all had a direct responsibility supporting their organizations in delivering compliance with U.S. federal government cybersecurity requirements as a supplier. This round employed multiple tools to process and analyze data. NVivo was utilized to explore open-ended survey questions and

provided the researcher with the tools needed to categorize the themes present in the participant responses. Once the themes were classified, the data was transferred out of NVivo and into Microsoft Excel. The identified themes were then further categorized in alignment with organizational culture theory levels, which are Artifacts, Beliefs, and Assumptions. All data charts and tables produced in this round were developed in Microsoft Excel. The following section presents the themes categorized under the organizational culture theory framework and the number of words coded for each question. The number of words coded corresponds to the specific sentence within a participant's response, where a theme was identified and categorized. After analyzing the responses to the first question within Round 1, "Explain your role as a cybersecurity leader?" the researcher identified themes that were further categorized under organizational culture theory. Figure 3 provides the analysis of the coded themes and the associated word count for each theme.

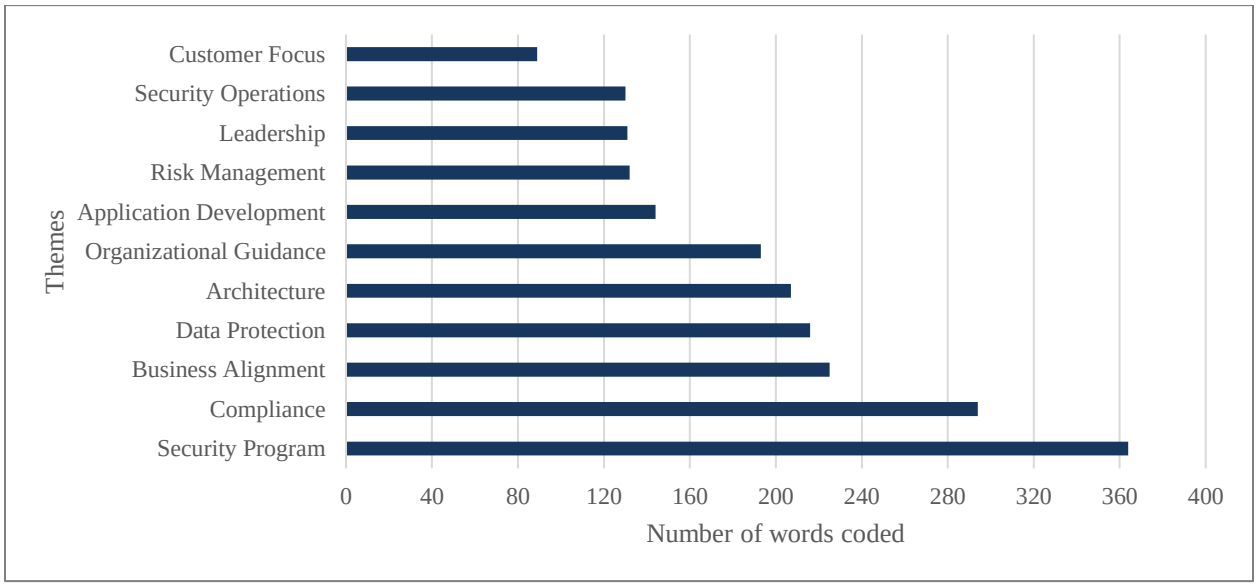

Figure 3. Themes Identified from Question 1 of Round 1

The word count Based on the analysis of question one from Round 1, (a) security program, (b) compliance, (c) business alignment, (d) data protection, and (e) architecture were the top five themes identified by panelists as it relates to the role of a cybersecurity leader. The themes that describe a cybersecurity leader's role when categorized against organizational culture theory are shown in Table 1. The Organizational Culture Theory levels of Artifacts and Assumptions were the top levels, which were equally represented with 24 references each. Beliefs were slightly less represented with 22 references making this the least referenced organizational culture theory level for this question. While Beliefs were the least represented, this level did contain the most significant sum of references related to the top five themes identified by panelists as it relates to the role of a cybersecurity leader.

Table 1

Summary of Responses from Question 1 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Architecture	7
	Security Operations	6
	Compliance	6
	Risk Management	5
Beliefs	Security Program	11
	Application Development	5
	Data Protection	6
Assumptions	Organizational Guidance	7
	Business Alignment	7

Categories	Identified Themes	Number of References
	Customer Focus	5
	Leadership	5

After analyzing the responses to the second question within Round 1, which was “Rank the below roles in order of importance for the CISO.” The rankings that were provided to the expert panel were “Business Partner and Integrator, Technical Security Operations, Security Architecture, Security Program Management, Governance and Compliance, Risk Management, Communications and Marketing, Strategy and Planning, and Security Knowledge.” The researcher analyzed the rankings and panelists responses from question two, which were then categorized under organizational culture theory. Figure 4 provides an analysis of the ranking. Based on the analysis of question two from Round 1, (a) risk management, (b) strategy and planning, (c) business partner and integrator, (d) governance and compliance, and (e) security knowledge were the top five roles identified by panelists as it relates to the role of the CISO.

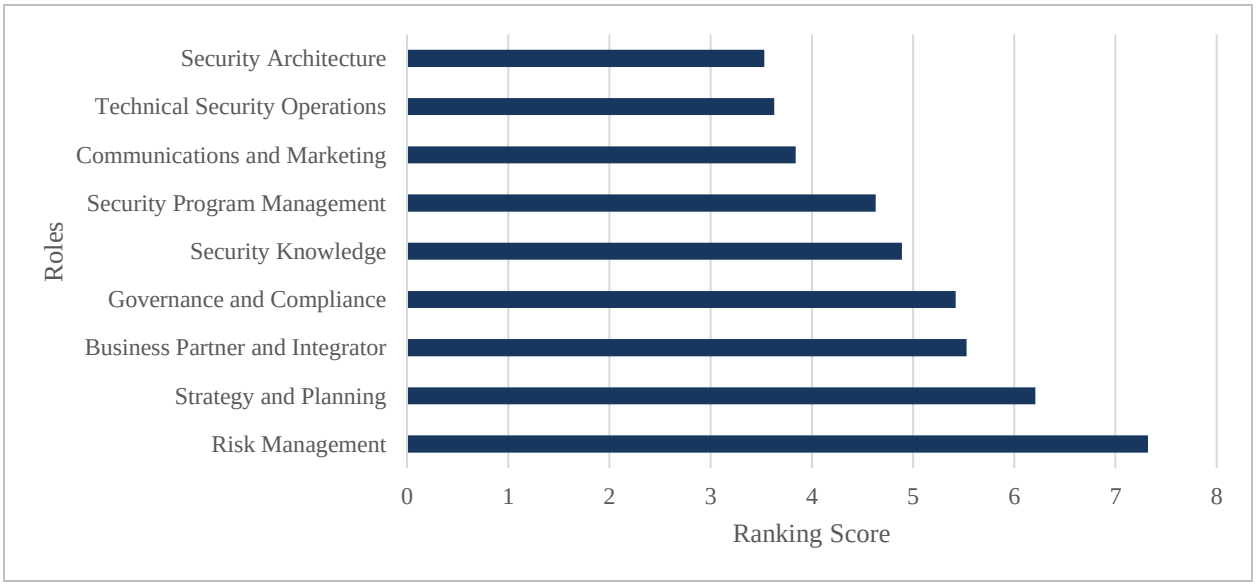

Figure 4. Ranking Score from Question 2 of Round 1

Expert 6 identified that "to be an effective CISO, you shift from being a mere technologist to a focused business leader that provides security as a value to the business." Expert 10 observed that "You must know the risks you face in real-time and know how to manage them." The roles of a cybersecurity leader when categorized against organizational culture theory are shown in Table 2. The Organizational Culture Theory level of Artifacts was the top-level identified with an overall ranking score of 16.27, followed by Beliefs with a score of 14.47 and, finally, assumptions with a score of 14.26. Artifacts contained the greatest score related to the top five roles identified by panelists as it relates to the roles in order of importance for the CISO.

Table 2

Summary of Rankings from Question 2 of Round 1

Categories	Identified Themes	Ranking Score
Artifacts	Risk Management	7.32
	Governance and Compliance	5.42
	Security Architecture	3.53
Beliefs	Strategy and Planning	6.21
	Security Program Management	4.63
	Technical Security Operations	3.63
Assumptions	Business Partner and Integrator	5.53
	Security Knowledge	4.89
	Communications and Marketing	3.84

After analyzing the responses to the third question within Round 1,“Define Business Partner and Integrator in your own words.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 2 noted that a “business partner and integrator enable the enterprise's core mission and processes with cybersecurity as a core tenant, while not disrupting or preventing operations.” Expert 13 stated that they “partner with internal corporate staff, external customers, and vendors to produce reliable, cost-effective security solutions.” Figure 5 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question three from Round 1, business relationship, (b) architecture, and (c) business alignment, (d) security program, and (e) business partners were the top five themes identified by panelists as it relates to the definition of a business partner and integrator.

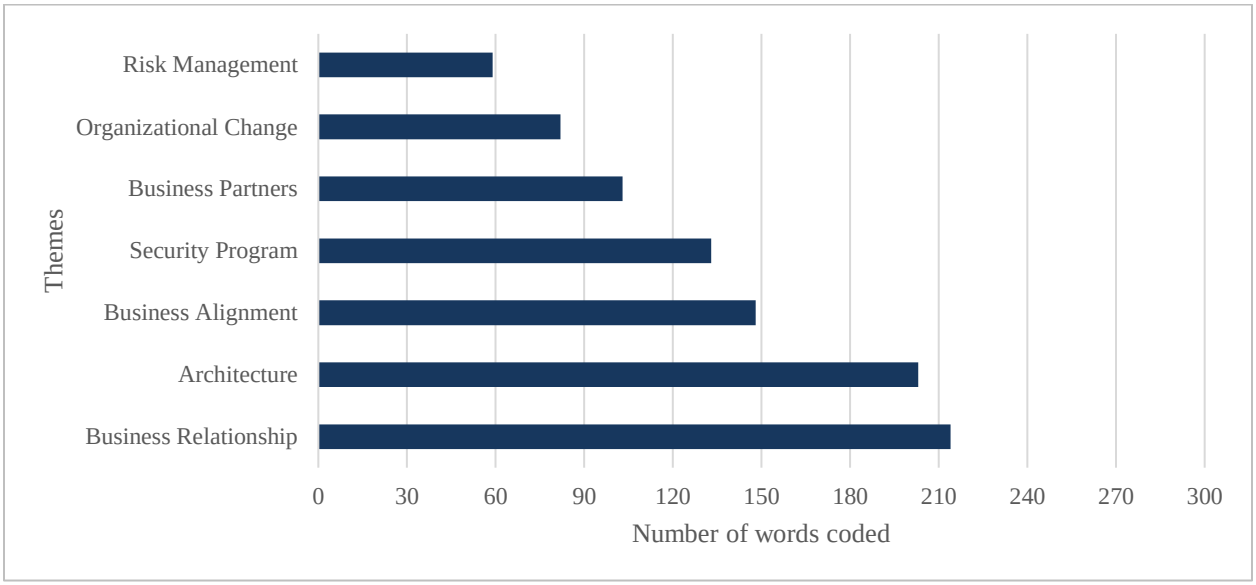

Figure 5. Themes Identified from Question 3 of Round 1

The themes related to business partner and integrator were then categorized against organizational culture theory, as shown in Table 3. The Organizational Culture Theory level of Assumptions was the top-level identified with 22 total references, followed by Artifacts with 11

references and finally, Beliefs with six references. Assumptions also contained the most significant score associated with the top five themes identified by panelists related to the topic of a business partner and integrator.

Table 3

Summary of Responses from Question 3 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Architecture	8
	Risk Management	3
Beliefs	Security Program	6
Assumptions	Business Relationship	9
	Business Alignment	5
	Organizational Change	4
	Business Partners	4

After analyzing the responses to the fourth question within Round 1, which was “Define Technical Security Operations in your own words.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 8 stated that technical security operations is “managing the enterprise's 24x7 operations by conducting automated monitoring to detect, analyze, and respond to cyber incidents.” Expert 19 identified technical security operations as the “ability to operate and lead security services that focus on operational delivery requiring technical depth, leadership, and business/mission alignment.” Figure 6 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question four from Round 1, (a) security operations, (b) security incidents, (c)

security program, (d) security tools, and (e) vulnerability management were the top five themes identified by panelists as it relates to the definition of technical security operations.

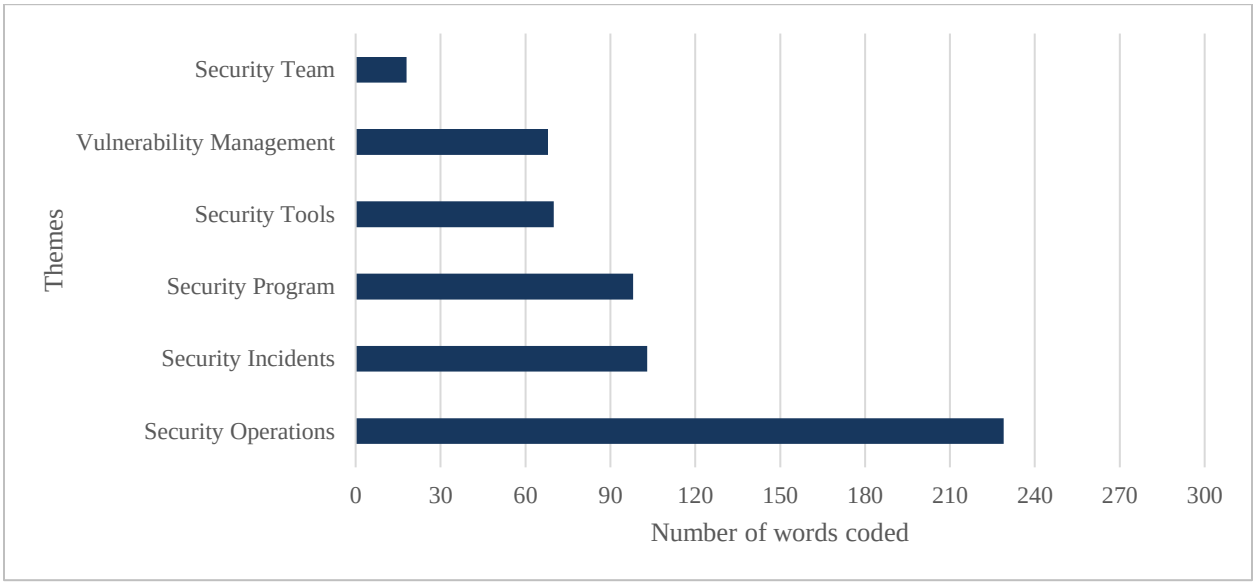

Figure 6. Themes Identified from Question 4 of Round 1

The themes related to technical security operations were then categorized against organizational culture theory, as shown in Table 4. The Organizational Culture Theory level of Artifacts was the top-level identified with 15 total references, followed by Beliefs with 13 references and finally, Assumptions with two references. Artifacts also contained the greatest score associated with the top five themes identified by panelists related to the topic of technical security operations.

Table 4

Summary of Responses from Question 4 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Security Operations	12
	Security Tools	3

Categories	Identified Themes	Number of References
Beliefs	Security Program	5
	Vulnerability Management	4
	Security Incidents	4
Assumptions	Security Team	2

After analyzing the responses to the fifth question within Round 1, which was “Define Security Architecture in your own words.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 10 stated that security architecture provides “the building blocks of the network that provide security in technology and policy terms.” Expert 14 identified that “security architecture is the design of systems and resources necessary to address security, privacy, and compliance concerns.” Figure 7 provides the analysis of the coded themes and word count for each theme.

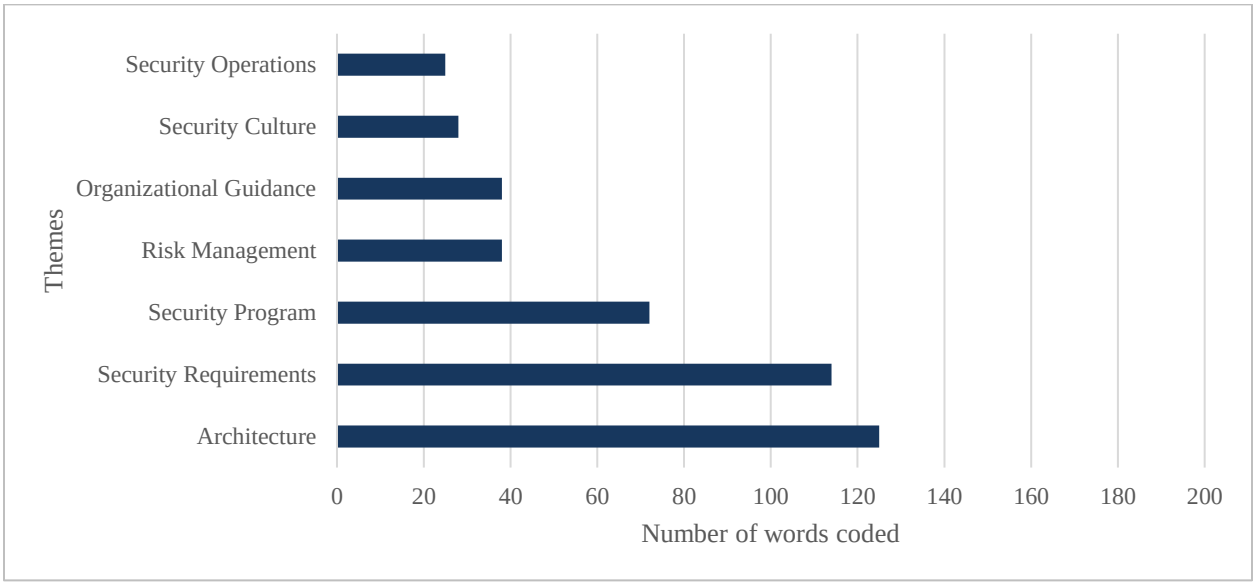

Figure 7. Themes Identified from Question 5 of Round 1

Based on the analysis of question five from Round 1, (a) architecture, (b) security requirements, (c) security program, (d) risk management, and (e) organizational guidance were the top five themes identified by panelists as it relates to the definition of security architecture. The themes related to security architecture were then categorized against organizational culture theory, as shown in Table 5. The Organizational Culture Theory level of Artifacts was the top-level identified with 14 total references, followed by Assumptions with four references and finally, Beliefs with three references. Artifacts also contained the greatest score associated with the top five themes identified by panelists related to the topic of security architecture.

Table 5

Themes Identified from Question 5 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Architecture	6
	Security Requirements	5
	Security Operations	2
	Risk Management	1
Beliefs	Security Program	3
Assumptions	Organizational Guidance	3
	Security Culture	1

After analyzing the responses to the sixth question within Round 1, “Define Security Program Management in your own words.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 2 noted that security program management includes “cost, schedule, performance (and measurement) of security

programs." Expert 8 stated that security program management "ensures that information security requirements, objectives, and policies are established and are integrated into the organization's processes from an enterprise-level down to programs and projects." Figure 8 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question six from Round 1, (a) program management, (b) project management, (c) security requirements, (d) architecture, and (e) security operations were the top five themes identified by panelists as it relates to the definition of security program management.

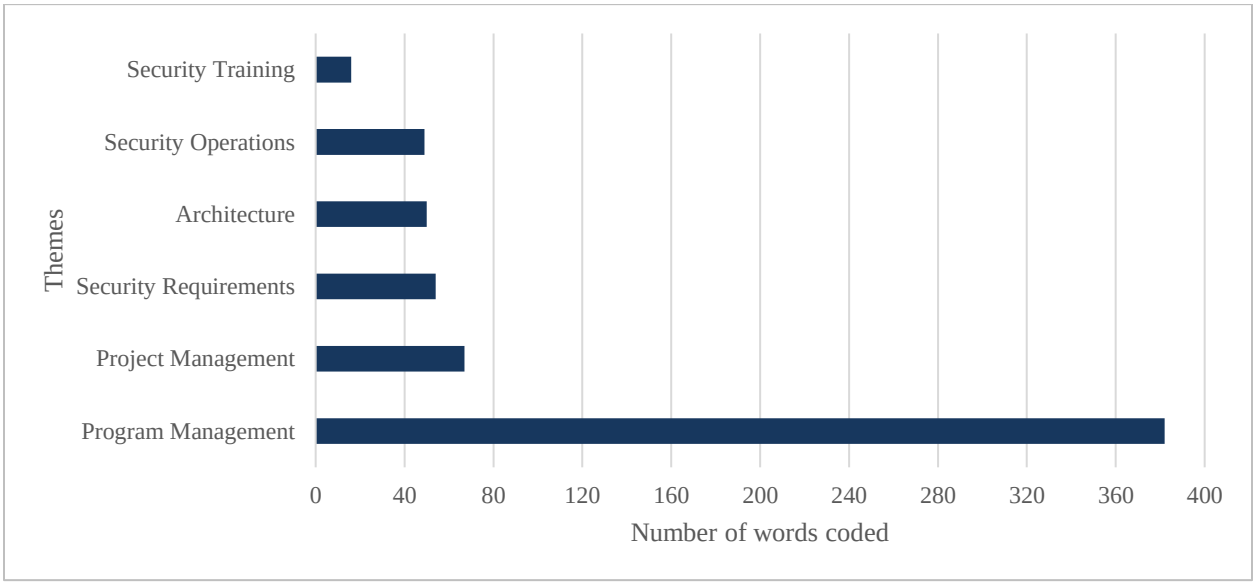

Figure 8. Themes Identified from Question 6 of Round 1

The themes related to security program management were then categorized against organizational culture theory, as shown in Table 6. The Organizational Culture Theory level of Beliefs was the top-level identified with 19 total references, followed by Artifacts with seven references and finally, Assumptions with one reference. Beliefs also contained the greatest score associated with the top five themes identified by panelists related to the topic of security architecture.

Table 6

Themes Identified from Question 6 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Security Requirements	3
	Security Operations	2
	Architecture	2
Beliefs	Program Management	15
	Project Management	4
Assumptions	Security Training	1

After analyzing the responses to the seventh question within Round 1, “Define Governance and Compliance in your own words.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 7 stated that “governance is all the requirements, procedures, policies, and standards for information security. Compliance describes how the business shows they align with contracts, regulations, policies, and laws. Expert 14 noted that “governance and compliance is a company's strategy for managing the broad issues of governance, risk management, and corporate compliance concerning risk and regulatory requirements.” Figure 9 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question seven from Round 1, (a) security requirements, (b) program management, (c) compliance, (d) security controls, and (e) risk management were the top five themes identified by panelists as it relates to the definition of governance and compliance.

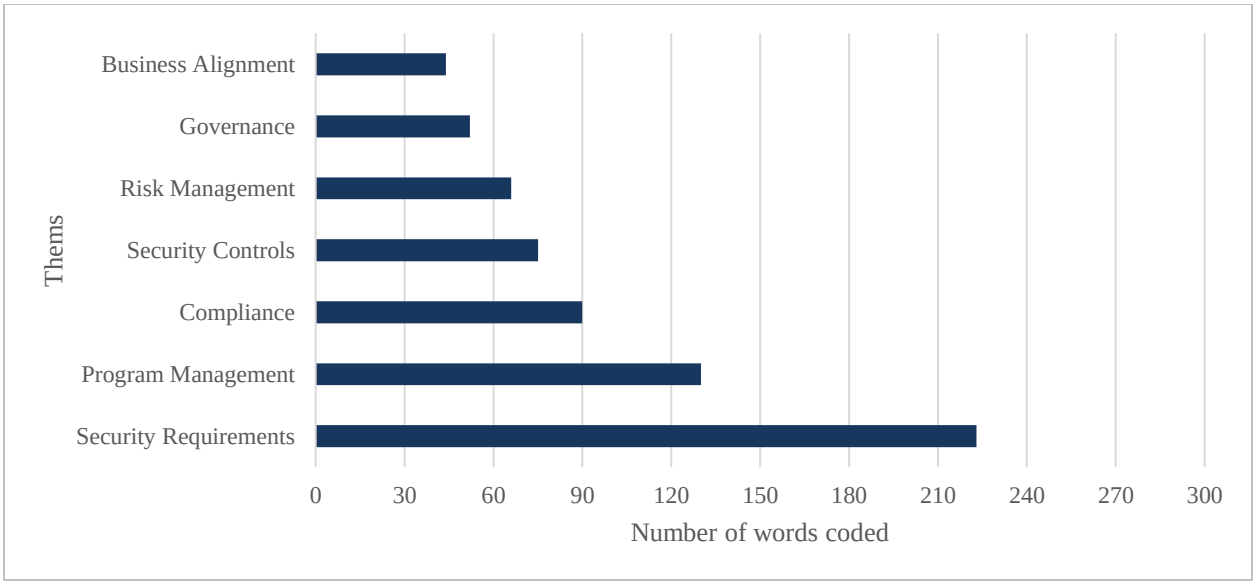

Figure 9. Themes Identified from Question 7 of Round 1

The themes related to governance and compliance were then categorized against organizational culture theory, as shown in Table 7. The Organizational Culture Theory level of Artifacts was the top-level identified with 22 total references, followed by Beliefs with five references and finally, Assumptions with two references. Artifacts also contained the greatest score associated with panelists' top five themes related to governance and compliance.

Table 7

Themes Identified from Question 7 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Security Requirements	9
	Governance	4
	Risk Management	3
	Security Controls	3
	Compliance	3

Categories	Identified Themes	Number of References
Beliefs	Program Management	5
Assumptions	Business Alignment	2

After analyzing the responses to the eighth question within Round 1, which was “Define Risk Management in your own words.” the researcher identified themes within the panelist's answers and categorized them under organizational culture theory. Expert 12 stated that “defining, enforcing, and documenting risk - is an effort to set and maintain a compliant (and operable) Risk Posture.” Expert 17 discussed that risk management is “the definition and actuarial analysis of top risks to revenue and profit, and the management of priorities among risks to which funds will be allocated for remediation.” Figure 10 provides the analysis of the coded themes and word count for each theme.

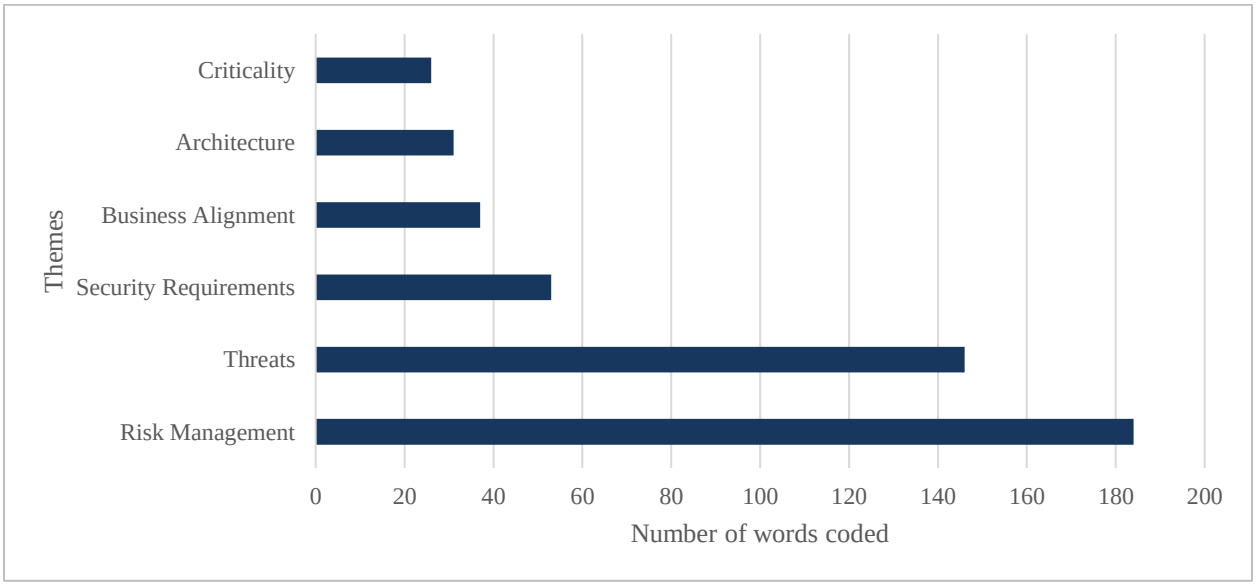

Figure 10. Themes Identified from Question 8 of Round 1

Based on the analysis of question eight from Round 1, (a) risk management, (b) threats, (c) security requirements, (d) business alignment, and (e) architecture were the top five themes

identified by panelists as it relates to the definition of risk management. The themes related to risk management were then categorized against organizational culture theory, as shown in Table 8. The Organizational Culture Theory level of Artifacts was the top-level identified with 13 total references, followed by Beliefs with eight references and finally, Assumptions with three references. Artifacts also contained the greatest score associated with panelists' top five themes related to risk management.

Table 8

Themes Identified from Question 8 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Risk Management	8
	Security Requirements	3
	Architecture	2
Beliefs	Threats	6
	Criticality	2
Assumptions	Business Alignment	3

After analyzing the responses to the ninth question within Round 1, which was “Define Communications and Marketing in your own words.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 4 stated that “communication and marketing is the hard work of ensuring that the org is clear on security's mission and how the things that we do tie into that mission. It requires talking about security and security risk in terms that most users can comprehend. Expert 13 discussed that “communications are directed both inwards and outwards to ensure a corporate culture of

security is maintained." Figure 11 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question nine from Round 1, (a) program management, (b) communications, (c) business alignment, (d) organizational change, and (e) security requirements were the top five themes identified by panelists as it relates to the definition of communication and marketing.

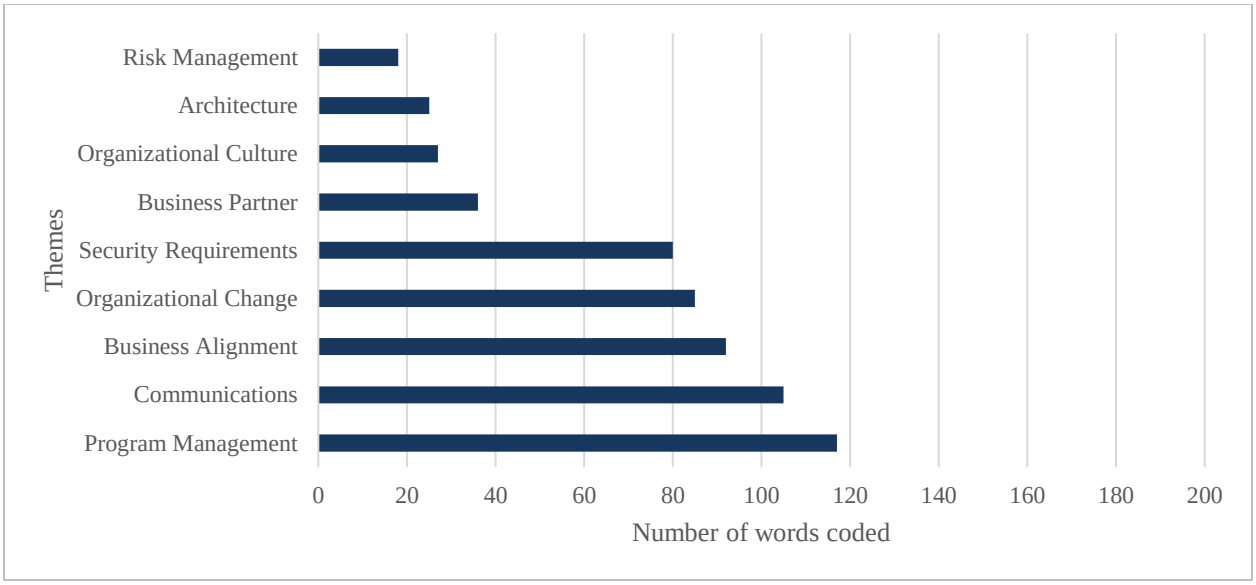

Figure 11. Themes Identified from Question 9 of Round 1

The themes related to communication and marketing were then categorized against organizational culture theory, as shown in Table 9. The Organizational Culture Theory level of Assumptions was the top-level identified with 11 total references, followed by Beliefs with ten references, and Artifacts with six references. Beliefs contained the greatest score associated with the top five themes identified by panelists related to the topic of communication and marketing.

Table 9

Themes Identified from Question 9 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Security Requirements	4
	Risk Management	1
	Architecture	1
Beliefs	Program Management	5
	Communications	5
Assumptions	Business Alignment	4
	Organizational Change	3
	Organizational Culture	2
	Business Partner	2

After analyzing the responses to the tenth question within Round 1, which was “Define Strategy and Planning in your own words.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 1 discussed that “strategy sets the direction, guiding principles, and goals for the program with planning focused on developing and implementing the specific elements of that strategy and accomplishing the stated goals. A cybersecurity strategy should focus on the needs of the business and protecting the information based on the value to the business.” Expert 15 identified that “strategy and planning includes taking a forward-looking view of what you want to accomplish, the current state of the security program, and the steps to achieve the target state.” Figure 12 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question

ten from Round 1, (a) business alignment, (b) program management, (c) architecture, (d) leadership, and (e) funding were the top five themes identified by panelists as it relates to the definition of strategy and planning.

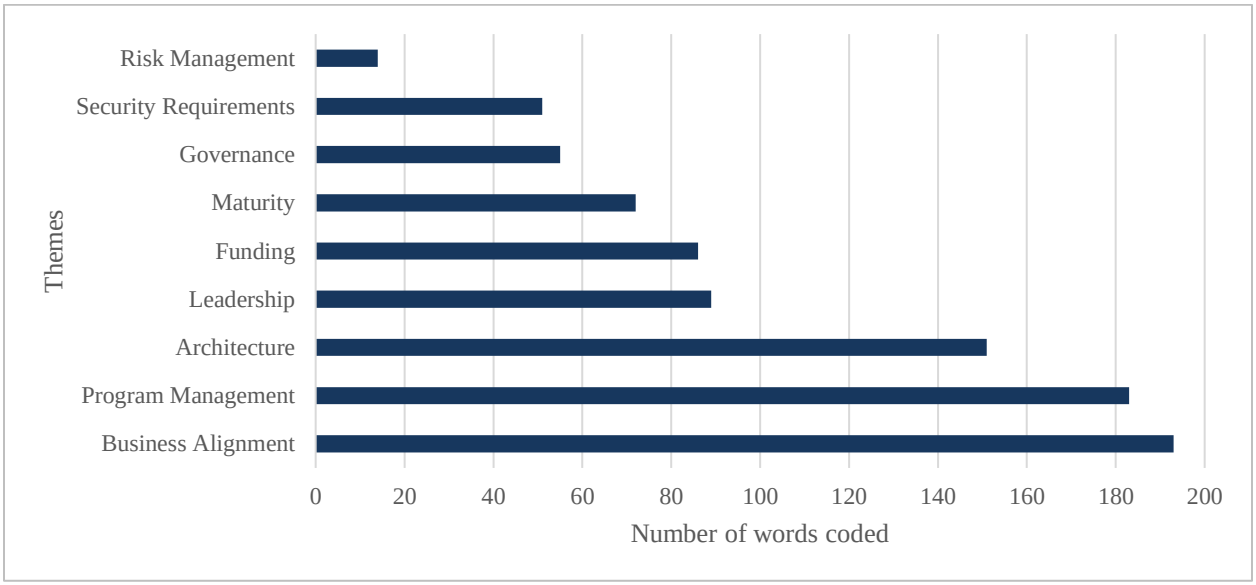

Figure 12. Themes Identified from Question 10 of Round 1

The themes related to strategy and planning were then categorized against organizational culture theory, as shown in Table 10. The Organizational Culture Theory level of Assumptions was the top-level identified with 14 total references, followed by Artifacts with 13 references and finally, Beliefs with seven references. Assumptions contained the greatest score associated with panelists' top five themes related to communication and marketing.

Table 10

Themes Identified from Question 10 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Security Requirements	3
	Architecture	5

Categories	Identified Themes	Number of References
	Funding	2
	Governance	2
	Risk Management	1
Beliefs	Program Management	7
Assumptions	Business Alignment	8
	Leadership	3
	Maturity	3

After analyzing the responses to the eleventh question within Round 1, which was "Define Security Knowledge in your own words." the researcher identified themes within the panelist's answers and categorized them under organizational culture theory. Expert 3 identified that security knowledge is the "overall understanding of current technologies, policy, and processes that can be applied to solve cybersecurity challenges." Expert 8 discussed "having the education and tactical/operational experience to lead a company in the right direction with the right priorities and focus" encompasses security knowledge. Figure 13 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question eleven from Round 1, (a) education and training, (b) program management, (c) security operations, (d) organizational guidance, and (e) risk management were the top five themes identified by panelists as it relates to the definition of security knowledge.

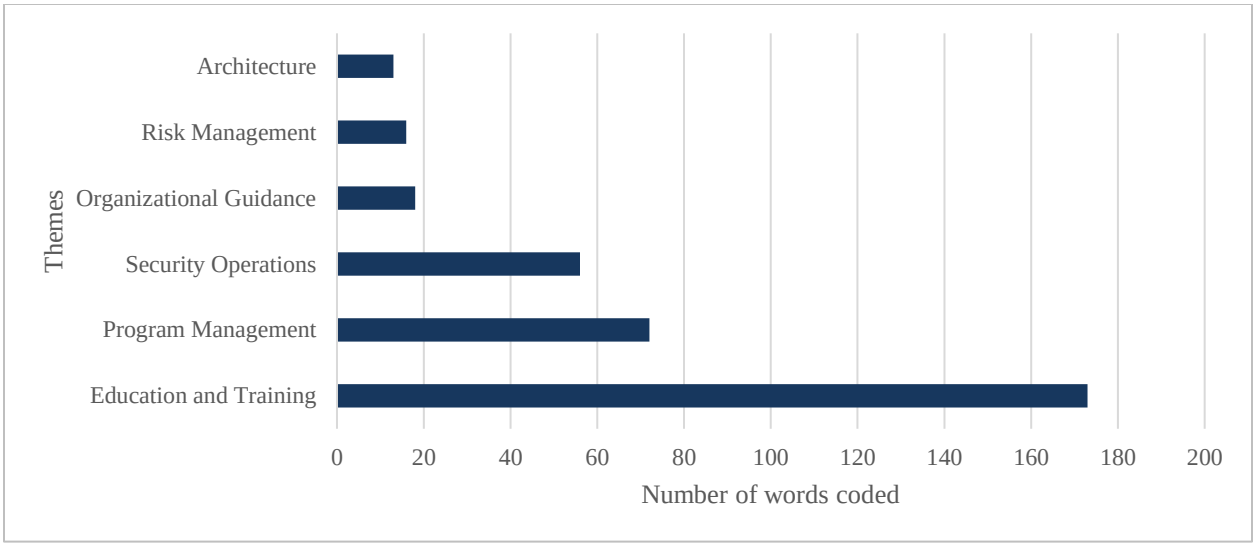

Figure 13. Themes Identified from Question 11 of Round 1

The themes related to security knowledge were then categorized against organizational culture theory, as shown in Table 11. The Organizational Culture Theory level of Assumptions was the top-level identified with ten total references, followed by Artifacts with four references and finally, Beliefs with three references. Assumptions contained the greatest score associated with the top five themes identified by panelists related to the topic of security knowledge.

Table 11

Themes Identified from Question 11 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Security Operations	2
	Architecture	1
	Risk Management	1
Beliefs	Program Management	3
Assumptions	Organizational Guidance	1
	Education and Training	9

After analyzing the responses to the twelfth question within Round 1, which was “For the top five roles identified in question one, describe why these roles made it into your list of top roles.” the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 3 stated that “security is about risk management and mitigation. You need to know what you have to comply with, what your business needs are, and have the knowledge to create a strategy and plan to address those needs.” Expert 9 discussed that “over the years, the role of a CISO has evolved into a risk manager. In assuming this responsibility, the leader must possess the knowledge and ability to identify risks for the organization and align security priorities based on risk mitigation objectives.” Figure 14 provides the analysis of the coded themes and word count for each theme.

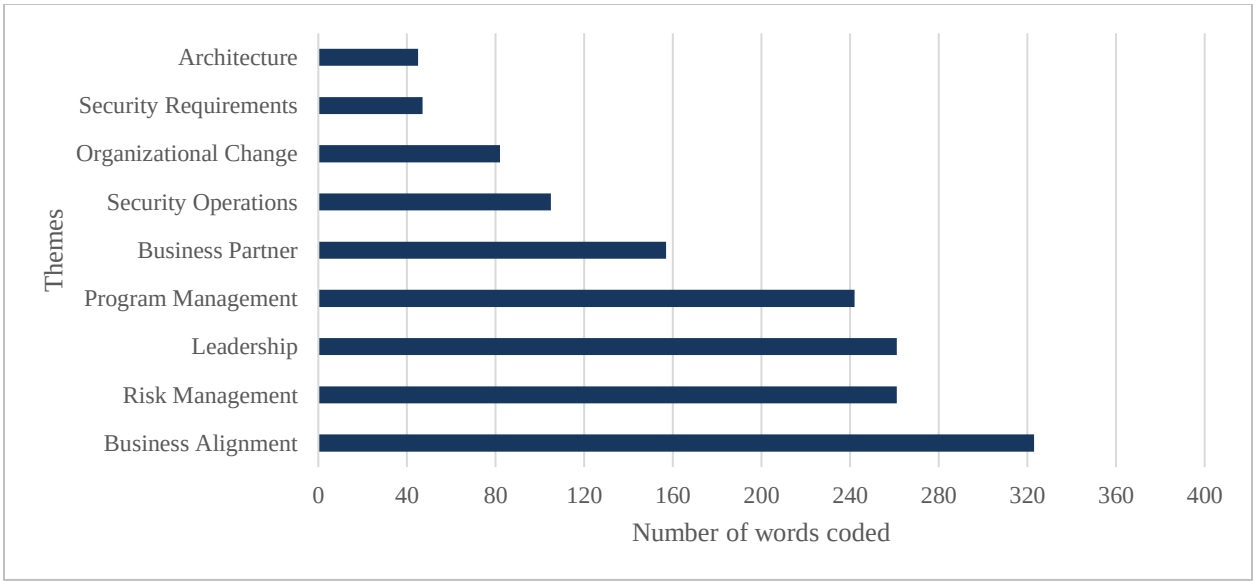

Figure 14. Themes Identified from Question 12 of Round 1

Based on the analysis of question 12 from Round 1, (a) business alignment, (b) risk management, (c) leadership, (d) program management, and (e) business partner were the top five themes identified by panelists as it relates to the reason that participants selected their top five roles. The themes related to security knowledge were then categorized against organizational

culture theory, as shown in Table 12. The Organizational Culture Theory level of Assumptions was the top-level identified with 34 total references, followed by Artifacts with 16 references and finally, Beliefs with eight references. Assumptions contained the greatest score associated with the top five themes identified by panelists related to the topic of security knowledge.

Table 12

Themes Identified from Question 12 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Risk Management	10
	Security Operations	3
	Security Requirements	2
	Architecture	1
Beliefs	Program Management	8
Assumptions	Business Alignment	13
	Leadership	11
	Business Partner	6
	Organizational Change	4

After analyzing the responses to the 13th question within Round 1, which was "Where should the CISO report within the organization to achieve the greatest effectiveness?" the researcher analyzed the data to understand where the participants believed the CISO should report to from a management relationship. Figure 15 provides the analysis of where the CISO should report managerially to achieve the most significant effects for the organization,

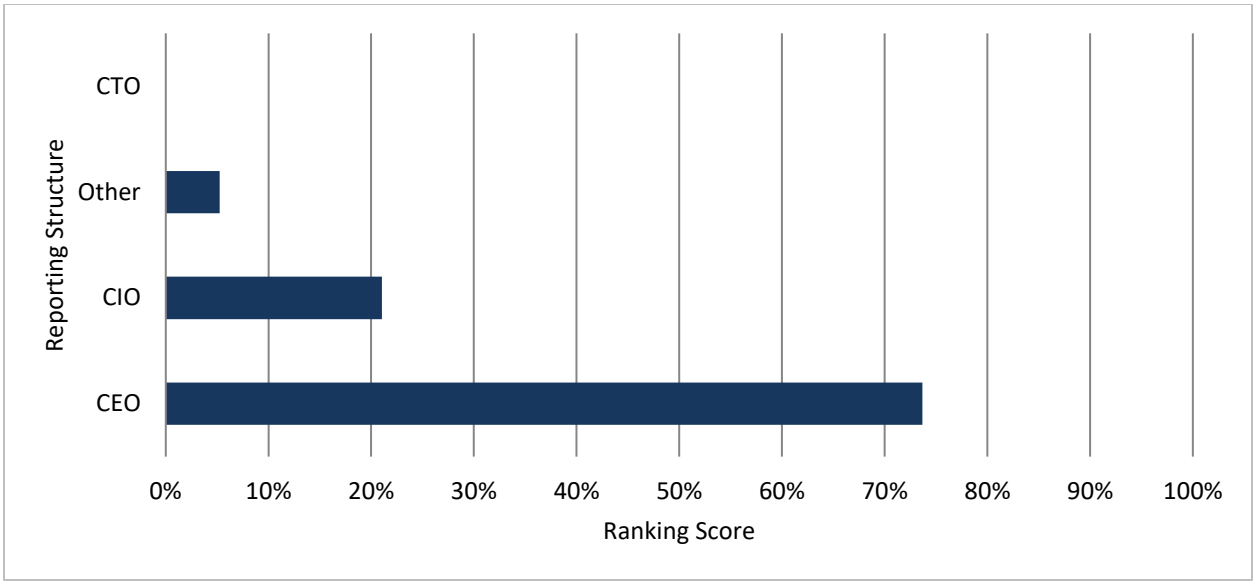

Figure 15. Reporting Structure Data Identified from Question 13 of Round 1

The Reporting Structure Data ranking scores are shown in Table 13.

Table 13

Reporting Structure Data Identified from Question 13 of Round 1

CISO Reporting Structure	Ranking Score
CEO	14
CIO	4
Other	1
CTO	0

After analyzing the responses to the 14th question within Round 1, which was "For your selection in question 13, please describe how this reporting structure will serve to contribute to the success of the CISO and security of the business?" the researcher identified themes that were then categorized under organizational culture theory. Expert 15 stated that "having a direct line of communication with the CEO allows the CISO to communicate risk and the state of the

program without intermediate filters that could have conflicts of interest." Expert 3 discussed that "the key to the CISO role is autonomy and accountability. I like the position in the CIO organization due to how closely the CISO has to work with the CIO." Figure 16 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question 14 from Round 1, (a) reporting accuracy, (b) business alignment, (c) program management, (d) organizational change, and (e) risk management were the top five themes identified by panelists as it relates to the reason that participants selected a specific reporting structure.

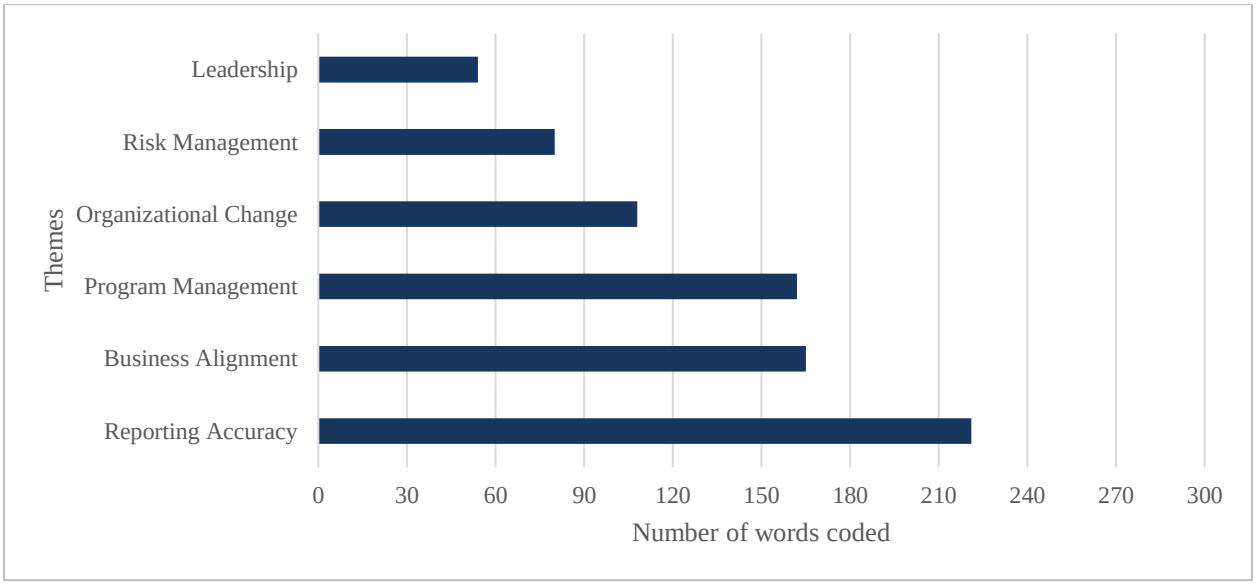

Figure 16. Themes Identified from Question 14 of Round 1

The themes related to a specific reporting structure for the CISO were then categorized against organizational culture theory, as shown in Table 14. The Organizational Culture Theory level of Beliefs was the top-level identified with 14 total references, followed by Assumptions with 13 references and finally, Artifacts with three references. Beliefs contained the greatest score associated with the top five themes identified by panelists related to the topic of security knowledge.

Table 14

Themes Identified from Question 14 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Risk Management	3
Beliefs	Program Management	6
	Reporting Accuracy	8
Assumptions	Organizational Change	4
	Business Alignment	7
	Leadership	2

After analyzing the responses to the 15th question within Round 1, which was "Is there any additional information you would like to provide related to the role of the CISO that will empower the CISO to succeed within an organization?" the researcher identified themes within the panelist's responses and categorized them under organizational culture theory. Expert 4 noted that "the mindset of partnering is a key component of success for CISO roles. Our recommendations will inevitably impede or slow down others' work progress as we try to secure our organization. Steer away from being perceived as the Office of No and focus on being an Organization of Enablement." Expert 8 discussed that "you must have the support and trust of the Executive Leadership team. You must continuously communicate with employees, and above all, always support the business in delivering secure solutions." Figure 17 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question 15 from Round 1, (a) business alignment, (b) program management, (c) threats, (d) training, and

(e) incident response were the top five themes identified by panelists as it related to additional information that the participants wished to convey.

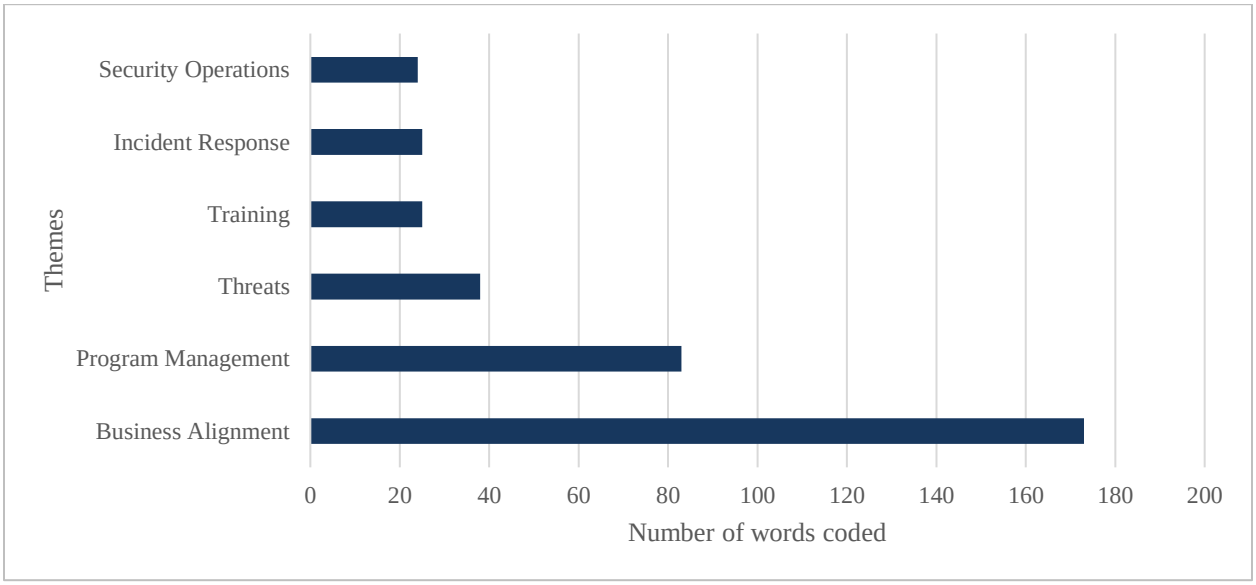

Figure 17. Themes Identified from Question 15 of Round 1

The themes related to additional information that the participants wished to convey were then categorized against organizational culture theory, as shown in Table 15. The Organizational Culture Theory level of Assumptions was the top-level identified with ten total references, followed by Beliefs with seven references, and finally, Artifacts with three references. Assumptions contained the greatest score associated with the top five themes identified by panelists related to the topic of security knowledge.

Table 15

Themes Identified from Question 15 of Round 1

Categories	Identified Themes	Number of References
Artifacts	Security Operations	2
	Incident Response	1

Categories	Identified Themes	Number of References
Beliefs	Program Management	5
	Threats	2
Assumptions	Business Alignment	9
	Training	1

The data analyzed from Round 1 revealed common themes used to establish the basis for the Round 2 questionnaire. The common themes and response data were used to construct definitions for the CISO roles ranked by the expert panel. This information was used in the remaining rounds to gain consensus from the expert panel related to what the specific roles mean and how they are applied within a government contracting organization. Figure 18 shows the top five themes identified across all of the questions in Round 1, which are (a) business alignment, (b) program management, (c) architecture, (d) risk management, and (e) security requirements.

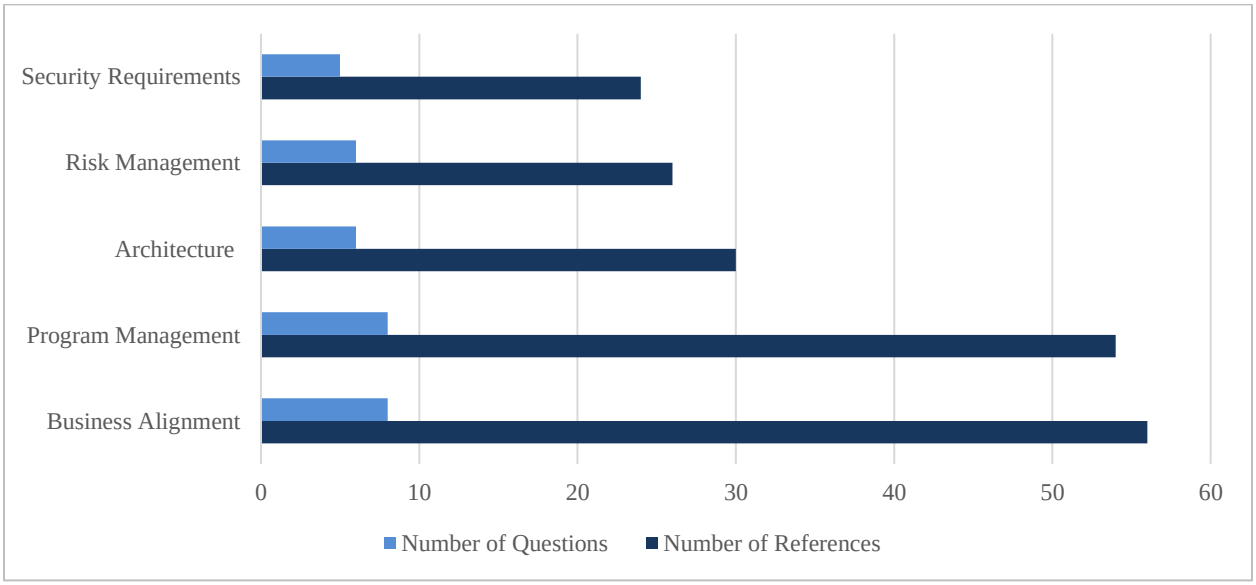

Figure 18. Top Five Themes Identified Within Round 1

Table 16 summarizes the top themes identified in Round 1, showing the number of references for each theme and the number of times a theme is present within a Round 1 question.

Table 16

Top Five Themes Identified Within Round 1

Themes	Number of References	Number of Questions
Business Alignment	56	8
Program Management	54	8
Architecture	30	6
Risk Management	26	6
Security Requirements	24	5

Figure 19 shows the distribution of themes across the levels of Organizational Culture Theory. Artifacts were the most often identified level, with 167 references. Assumptions were the second most used level, with 164 references. Finally, Beliefs was the least categorized level with 139 references.

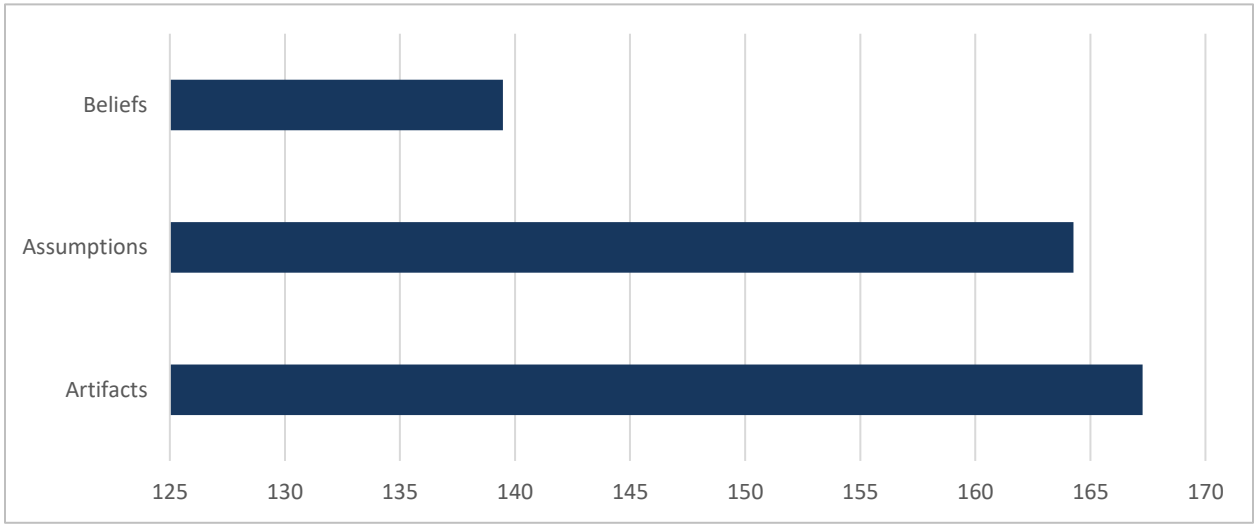

Figure 19. Organizational Culture Theory Summary for Round 1

Table 17 summarizes the distribution of theme references across the levels of Organizational Culture Theory that are present within Round 1.

Table 17

Organizational Culture Theory Summary for Round 1

Levels	Number of References
Artifacts	167
Assumptions	164
Beliefs	139

Once the data analysis concluded for Round 1, the researcher synthesized the participant's information to create the Round 2 questions. Round 2 continues to gain consensus on the role of the CISO. Based on the data provided by the participants and synthesized by the researcher, Round 2 served to achieve consensus on the definition of the roles by the expert panel.

Data Analysis Round 2

The expert panel's themes and data provided the information necessary to prepare the Round 2 questionnaire. The Round 2 questionnaire was utilized to gain additional consensus on the roles and reporting structure of the CISO. Also, in Round 2, definitions for the roles being ranked by the expert panel are introduced. The researcher developed the definitions through a careful analysis of the participant responses and the themes identified in the Round 1 survey. Round 2 of the study began on August 18, 2020, and ended on August 24, 2020. The Round 2 questions consisted mostly of closed-ended questions looking for consensus from the panelists related to the content being presented in each question. Microsoft Excel was used to analyze and present the data from all closed-ended questions. For the open-ended questions, a combination of

NVivo and Microsoft Excel was used. Thematic analysis was conducted in NVivo. Once the thematic analysis was completed, the data was moved to Excel for editing.

The first question in Round 2 asked the participants to determine if they agreed with the ranking presented to them related to the roles needed by the CISO to be successful within a government contracting organization. Table 18 shows the re-ranking of the roles based on participant feedback given in Round 1.

Table 18

ReRanking of Roles Based on Round 1 Feedback

Round 1	**Round 2**
Business Partner and Integrator	Risk Management
Technical Security Operations	Governance and Compliance
Security Architecture	Security Architecture
Security Program Management	Strategy and Planning
Governance and Compliance	Security Program Management
Risk Management	Technical Security Operations
Communications and Marketing	Business Partner and Integrator
Strategy and Planning	Security Knowledge
Security Knowledge	Communications and Marketing

The new list of roles was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 20 shows the participants' responses to this question, showing that there is no consensus for question one.

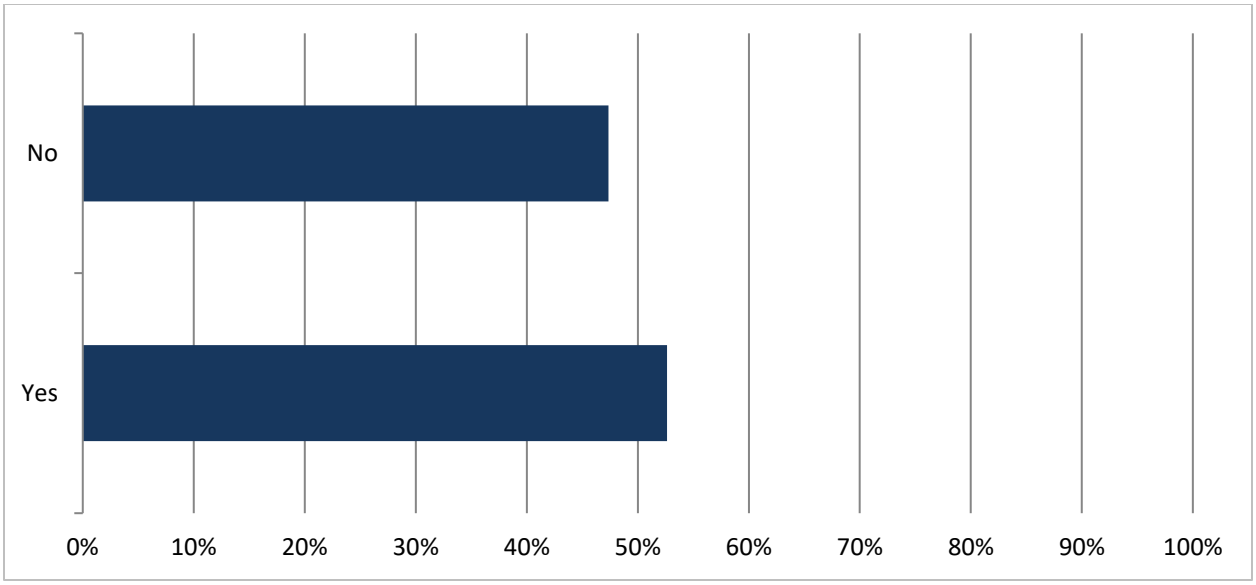

Figure 20. Responses from Question 1 of Round 2

Table 19 provides a summary analysis of the respondent's answers to question one. The participants provided nine total comments corresponding to the no responses to this question. These responses allowed the researcher to reorder the roles for use in the Round 3 questionnaire.

Table 19

Responses from Question 1 of Round 2

Question Response	Response Percentage	Number of Respondents
Yes	52.63%	10
No	47.37%	9

In Round 2, the second question asked the participants if they agreed with the definition of business partner and integrator developed based on the expert panels Round 1 response. The following is the definition provided for the panel's review "Someone that understands business priorities and challenges so that security is an enabler. They can communicate and partner with members of the business to achieve objectives securely and safely aligned with organizational

risk appetite. Business partners and integrators help to address gaps and augment organizational capabilities participating in discussions related to the connection of systems and the flow of business data bringing oversight, monitoring, and secure implementation capabilities to an engagement."

A business partner and integrator's definition was presented to the participants in this question to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 21 shows the participants' responses to this question, showing that there is consensus for question two amongst the panel of experts.

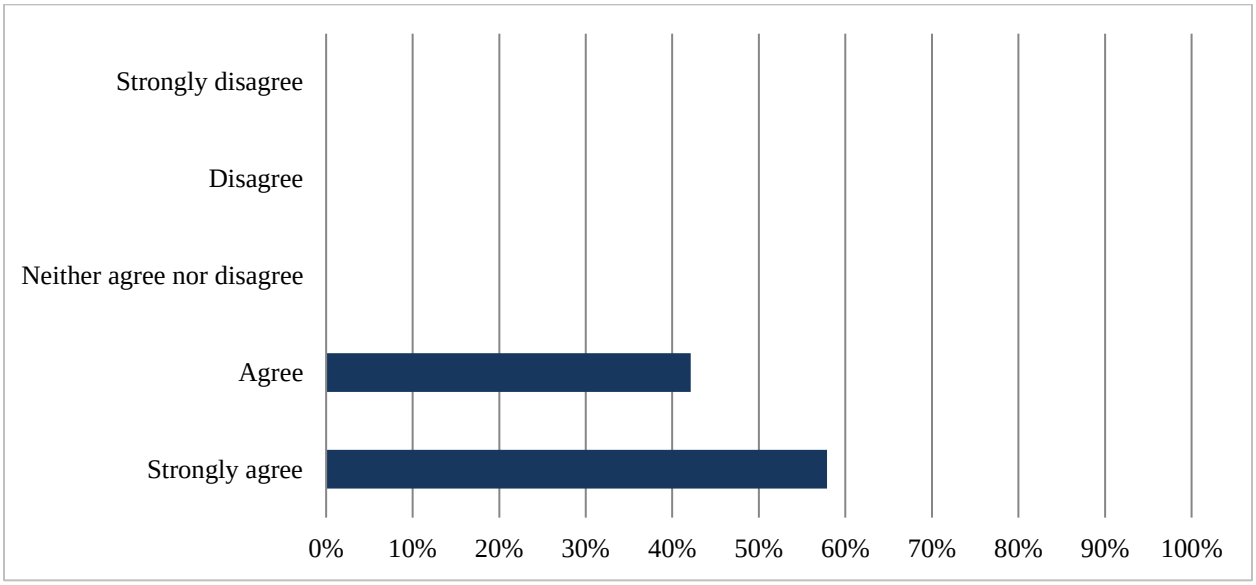

Figure 21. Responses from Question 2 of Round 2

While consensus exists for this question and definition, expert 1 stated that "business partners are those internal and external people or groups that own or support components of the business and join the CISO in the common cause of information security. Expert 4 discussed that "In my opinion security is only as successful as the business is. To achieve this, we need to align our security objectives with business goals." Table 20 provides a summary analysis of the

respondent's answers to question two. As consensus was reached for this question, this definition was not included in the Round 3 survey.

Table 20

Responses from Question 2 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	57.89%	11
Agree	42.11%	8
Neither agree nor disagree	0.00%	0
Disagree	0.00%	0
Strongly disagree	0.00%	0

The third question in Round 2 asked the participants if they agreed with the definition of technical security operations developed based on the expert panels Round 1 response. The following is the definition that was provided for the panel's review "Technical security operations are the day-to-day maintenance, management, and monitoring of incident response, threat hunting, vulnerability assessment, penetration testing/red teaming, forensics, and disaster recovery services for an organization allowing for risk to be managed to acceptable levels in support of organizational risk management and compliance requirements. This capability requires technical depth, leadership, and business/mission alignment with the ability to operate and lead security services that focus on operational delivery."

The definition of technical security operations was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content

acceptable. Figure 22 shows the participants' responses to this question, showing consensus does not exist for question three amongst the panel of experts. The participants provided comments allowing the researcher to improve the definition for use in the Round 3 questionnaire. Expert 8 explained that technical security operations is “managing the 24x7 operations of the Enterprise by conducting automated monitoring to detect, analyze and respond to cyber incidents using a combination of tools employing strong, repeatable processes.” Expert 14 noted that “security operations are concerned with the day-to-day management of resources responsible for security, privacy, and compliance.”

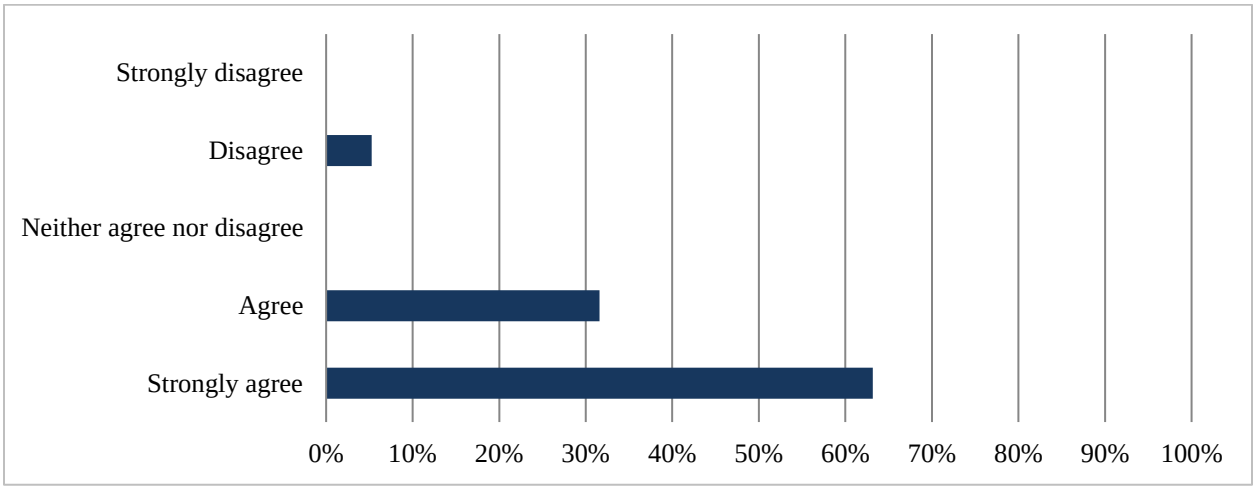

Figure 22. Responses from Question 3 of Round 2

Table 21 provides a summary analysis of the respondent’s answers to question three. Consensus was not reached for this question and the definition of technical security operations. The comment provided by the respondent allowed the researcher to improve the definition of technical security operations for use in the Round 3 questionnaire.

Table 21

Responses from Question 3 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	63.16%	12
Agree	31.58%	6
Neither agree nor disagree	0.00%	0
Disagree	5.26%	1
Strongly disagree	0.00%	0

The fourth question in Round 2 asked the participants if they agreed with the definition of security architecture developed based on the expert panels Round 1 response. The following is the definition that was provided for the panels review "Ability to define a framework and plan to implement an architecture and corporate security culture which decreases operational risk, enhances organizational security, and provides security standards for an organization's digital systems and components to address security, privacy, and compliance concerns. Security architecture requires one to think broadly about the interplay of various technology pieces as they develop technical blueprints, which allow for secure solution implementation supporting continuous security monitoring."

The definition of security architecture was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 23 shows the participants' responses to this question showing that there is consensus for question two amongst the panel of experts.

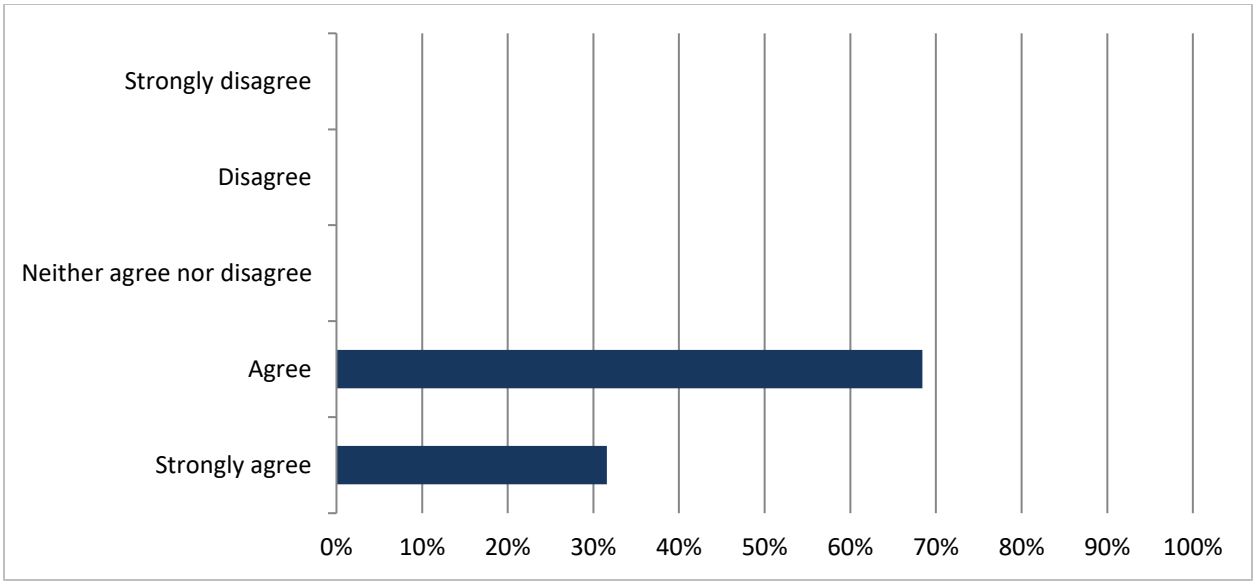

Figure 23. Responses from Question 4 of Round 2

While consensus exists for this question and definition, expert 8 stated that security architecture is "providing cybersecurity engineering and architecture support and standards to all projects and programs across the enterprise providing guidance and discipline to implement the cybersecurity requirements outlined by policy and regulatory compliance." Expert 16 discussed that "security architecture is the ability to think broadly about the interplay of various pieces of technology to ensure secure operation." Table 22 provides a summary analysis of the respondent's answers to question four. As consensus was reached for this question and the definition of security architecture, this definition was not included in the Round 3 survey.

Table 22

Responses from Question 4 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	31.58%	6
Agree	68.42%	13

Question Response	Response Percentage	Number of Respondents
Neither agree nor disagree	0.00%	0
Disagree	0.00%	0
Strongly disagree	0.00%	0

The fifth question in Round 2 asked the participants if they agreed with the definition of security program management developed based on the expert panels Round 1 response. The following is the definition that was provided for the panel's review “The leadership (regular, active management) of a program which provides operational roadmaps, security resources, and standards for an organization, in addition to operational capabilities that ensure the selection and implementation of management, operational, and technical security controls commensurate with both the risk and regulatory requirements of the enterprise. Security program management also encompasses the projects, programs, and portfolio management of security-related initiatives that support compliance, risk management, POAM resolution, technology development, policies/procedures, training, and funding which are coordinated to produce a resilient organization.”

The definition of security program management was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 24 shows the participants' responses to this question, showing a consensus for question two amongst the panel of experts.

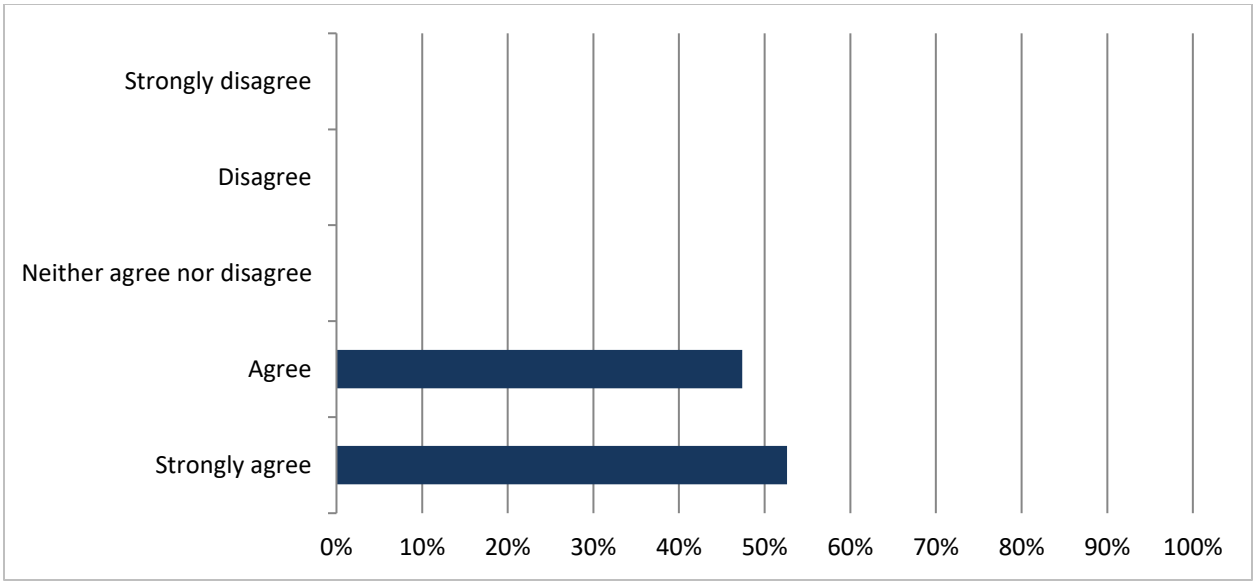

Figure 24. Responses from Question 5 of Round 2

While consensus exists for this question and definition Expert 9 stated that "security program management can be defined as accountability for delivering chartered responsibilities as established for the security function." Expert 14 explained that "security program management is understanding and managing information security, privacy, and risk selecting and implementing controls commensurate with both the risk and regulatory requirements." Table 23 provides a summary analysis of the respondent's answers to question five. As consensus was reached for this question and the definition of security program management, this definition was not included in the Round 3 survey.

Table 23

Responses from Question 5 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	52.63%	10
Agree	36.84%	7

Question Response	Response Percentage	Number of Respondents
Neither agree nor disagree	10.53%	2
Disagree	0.00%	0
Strongly disagree	0.00%	0

In Round 2, the sixth question asked the participants if they agreed with the definition of governance and compliance developed based on the expert panels Round 1 response. The following is the definition that was provided for the panel's review “A company's strategy for managing the broad issues of governance, risk management, and corporate compliance with all relevant federal, state, and local regulatory compliance requirements. This includes ensuring that stakeholder, legal, regulatory, and contractual requirements are evaluated, understood, and implemented as part of a security program and systems implementation.”

The definition of governance and compliance was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 25 shows the participants' responses to this question showing that consensus was not reached for question six amongst the panel of experts. The participants provided comments allowing the researcher to improve the definition for use in the Round 3 questionnaire. Expert 2 explained that “Governance, Risk, and Compliance, as a discipline, manages the governance processes and procedures across the enterprise.” Expert 8 stated that “governance and compliance are developing, documenting, implementing and continuously improving a company wide information security program to provide security for all systems, networks, and data that support the organization's operations.”

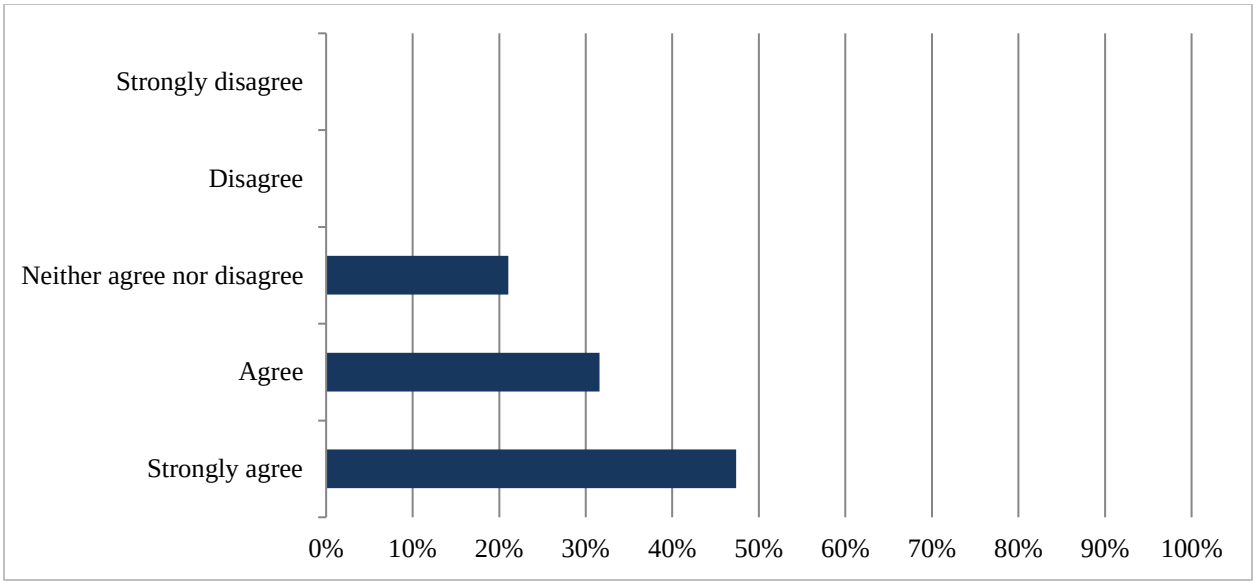

Figure 25. Responses from Question 6 of Round 2

Table 24 provides a summary analysis of the respondent's answers to question six. Consensus was not reached for this question and the definition of governance and compliance. The comments provided by the respondents allowed the researcher to improve the definition of governance and compliance for use in the Round 3 questionnaire.

Table 24

Responses from Question 6 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	47.37%	9
Agree	31.58%	6
Neither agree nor disagree	21.05%	4
Disagree	0.00%	0
Strongly disagree	0.00%	0

The seventh question in Round 2 asked the participants if they agreed with the definition of risk management developed based on the expert panels Round 1 response. The following is the definition that was provided for the panel's review “Defining and analyzing top risks to revenue, profit, and competitiveness for an organization working to manage priorities among risks to which funds will be allocated for remediation. This includes developing, operating, and leading while defining, enforcing, and documenting risk - to set and maintain a compliant (and operable) risk posture for the organization. Treatment plans are developed to address risks that are outside of the risk appetite of the organization based on a careful evaluation of threat actors, actor motivation, threats, threat likelihood, vulnerabilities, asset value, asset criticality, and the impact on a system, the organization, or the public. Not all risk can be eliminated from any given environment. The goal of Risk Management is to reduce risk to an acceptable level where the residual risk can be measured and is in alignment with management expectations.”

The definition of risk management was presented to the participants in this question to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 26 shows the participants' responses to this question showing that consensus was not reached for question seven amongst the panel of experts. The participants provided comments allowing the researcher to improve the definition for use in the Round 3 questionnaire. Expert 8 discussed that “having visibility across the entire company related to technology initiatives and activities and understanding the threat to all areas of the business, remediating discovered vulnerabilities can reduce the risk of the company.” Expert 14 started that “risk management is the management and mitigation of risks that potentially hinder an organizations operations or ability to remain competitive.”

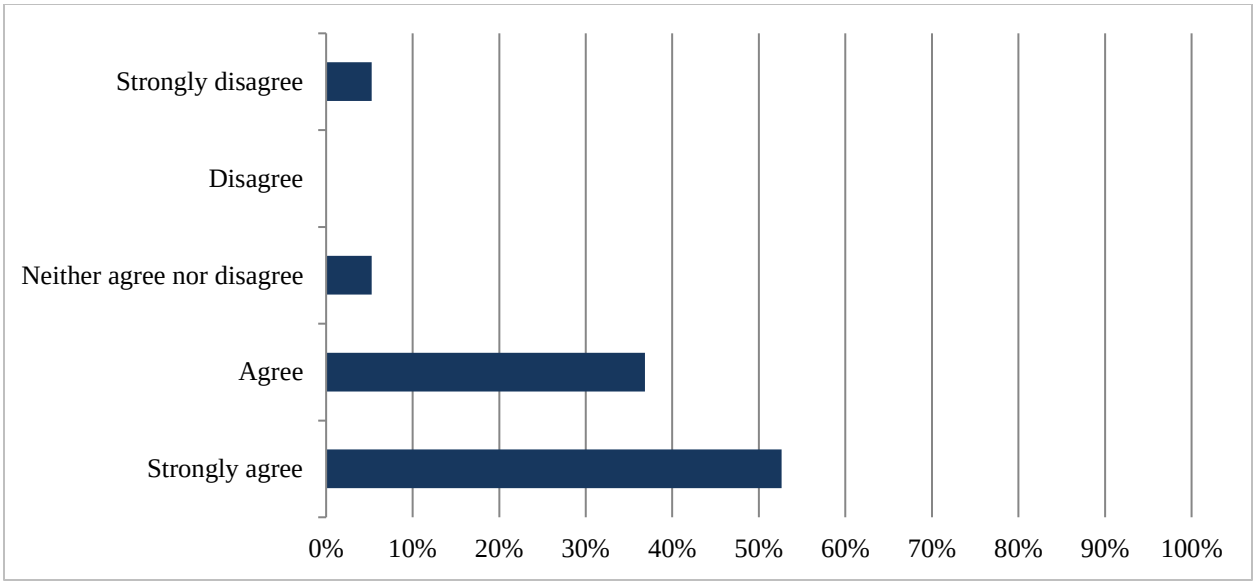

Figure 26. Responses from Question 7 of Round 2

Table 25 provides a summary analysis of the respondent's answers to question seven. Consensus was not reached for this question and the definition of risk management. The comments provided by the respondents allowed the researcher to improve the definition of risk management for use in the Round 3 questionnaire.

Table 25

Responses from Question 7 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	52.63%	10
Agree	36.84%	7
Neither agree nor disagree	5.26%	1
Disagree	0.00%	0
Strongly disagree	5.26%	1

The eighth question in Round 2 asked the participants if they agreed with the definition of communication and marketing developed based on the expert panels Round 1 response. The following is the definition that was provided for the panel's review “Evangelizing and disbursing information and ideas to establish buy-in at all organizational levels, about the organization’s security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis. The ability to communicate with business stakeholders about the importance and value of security considerations and market the business enabler that a sound security program provides for an organization. Communications and marketing are directed at all levels of the organization to ensure a corporate culture of security is developed and maintained.”

The definition of communication and marketing was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 27 shows the participants' responses to this question showing that consensus was not reached for question eight amongst the panel of experts. The participants provided comments allowing the researcher to improve the definition for use in the Round 3 questionnaire. Expert 7 noted that “communications and marketing have to do with how we interact with our customers / clients both internally and externally. Whether through an awareness video, email campaign, posters or even PR work.” Expert 17 discussed that “communication and marketing the ability to describe the security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis.”

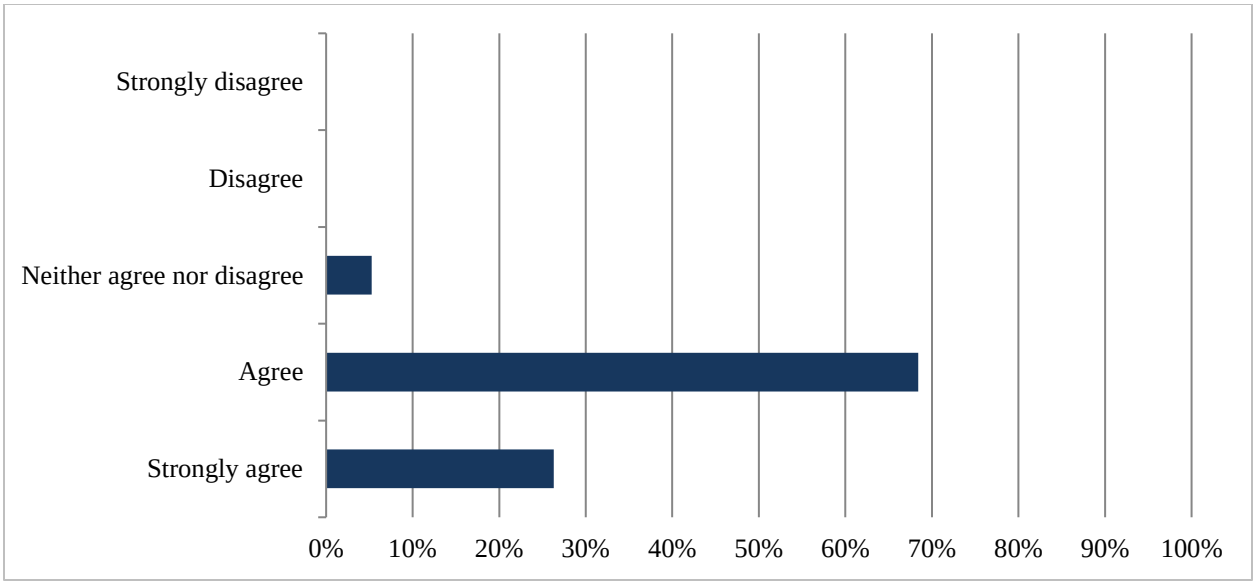

Figure 27. Responses from Question 8 of Round 2

Table 26 provides a summary analysis of the respondent's answers to question eight. Consensus was not reached for this question and the definition of communication and marketing. The comments provided by the respondents allowed the researcher to improve the definition of risk management for use in the Round 3 questionnaire.

Table 26

Responses from Question 8 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	26.32%	5
Agree	68.42%	13
Neither agree nor disagree	5.26%	1
Disagree	0.00%	0
Strongly disagree	0.00%	0

In Round 2, the ninth question asked the participants if they agreed with the definition of strategy and planning that was developed based on the expert panels Round 1 response. The following is the definition that was provided for the panel's review “A forward-looking view of the current state of the security program, what needs to be accomplished, and the steps to achieve a target state. This is achieved by analyzing the business's needs and setting appropriate goals and objectives that serve to deliver the security program’s target state via well-developed security plans that are easily understood by business leaders. By aligning corporate goals with those of the security program, a vision and path forward are promoted that are aligned and integrated with the mission of the business.”

The definition of strategy and planning was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 28 shows the participants' responses to this question showing that consensus was not reached for question nine amongst the panel of experts. The participants provided comments allowing the researcher to improve the definition for use in the Round 3 questionnaire. Expert 2 stated that “continuous transformation and optimization of the enterprise's cybersecurity and risk management posture supports strategy and planning.” Expert 7 explained that “strategy and planning takes into account near, medium, and far looking vision for the security organization taking into consideration, budgeting, resources, growth, and the overall business strategy.”

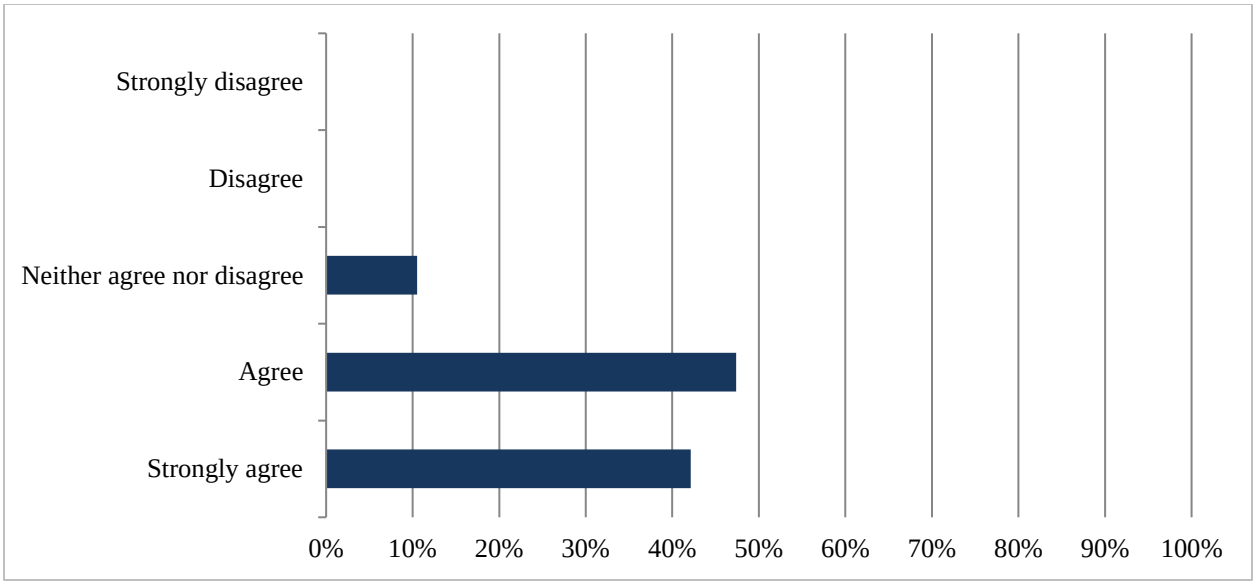

Figure 28. Responses from Question 9 of Round 2

Table 27 provides a summary analysis of the respondent's answers to question nine. Consensus was not reached for this question and the definition of strategy and planning. The comments provided by the respondents allowed the researcher to improve the definition of strategy and planning for use in the Round 3 questionnaire.

Table 27

Responses from Question 9 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	42.11%	8
Agree	47.37%	9
Neither agree nor disagree	10.53%	2
Disagree	0.00%	0
Strongly disagree	0.00%	0

In Round 2, the tenth question asked the participants if they agreed with the definition of security knowledge developed based on the expert panels Round 1 response. The following is the definition provided for the panel's review "Ability to understand technical security issues and concerns in conjunction with business operations considering risks and requirements that an organization has concerning security, privacy, and compliance. Having the expertise and technical background to implement a security posture that is triaged from a risk management perspective and considers the complexity and interconnectivity of the enterprise environment to maintain the business in a secure, compliant, and operational manner."

The definition of security knowledge was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 29 shows the participants' responses to this question showing that consensus was not reached for question nine amongst the panel of experts.

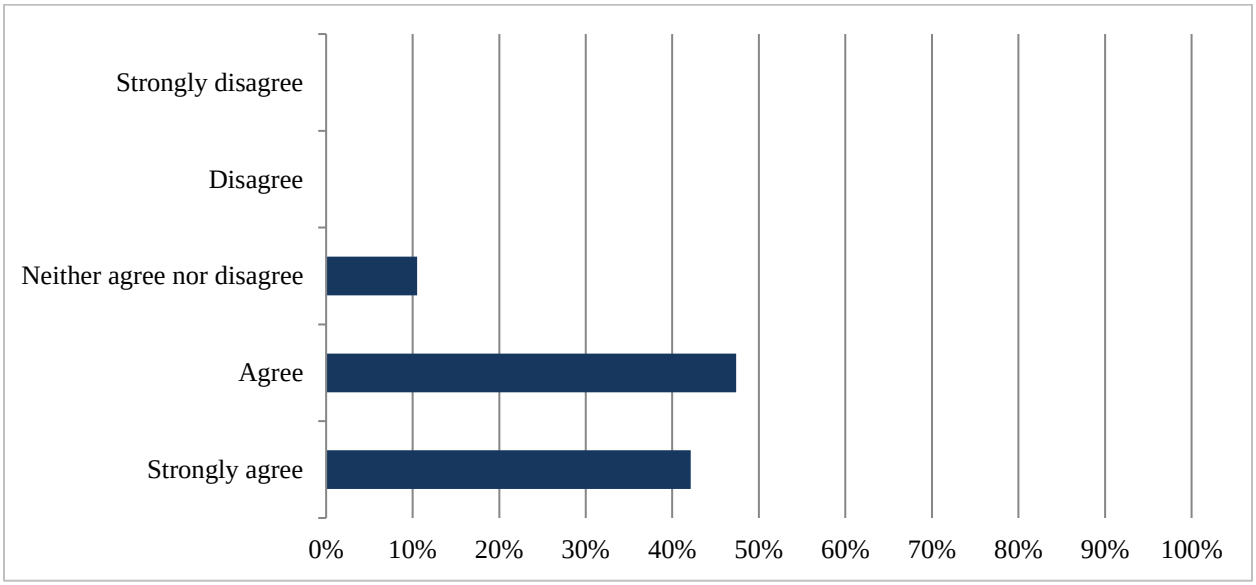

Figure 29. Responses from Question 10 of Round 2

The participants provided comments allowing the researcher to improve the definition for use in the Round 3 questionnaire. Expert 13 stated that "security knowledge is a function of training, both individual and organization-wide. Expert 17 discussed that "understanding the numerous systems deployed in common enterprise environments, the ways in which they interact, and the manners in which they are individually and systemically vulnerable to compromise comprises security knowledge." Table 28 provides a summary analysis of the respondent's answers to question ten. Consensus was not reached for this question and the definition of security knowledge. The comments provided by the respondents allowed the researcher to improve the definition of security knowledge for use in the Round 3 questionnaire.

Table 28

Responses from Question 10 of Round 2

Question Response	Response Percentage	Number of Respondents
Strongly agree	42.11%	8
Agree	47.37%	9
Neither agree nor disagree	10.53%	2
Disagree	0.00%	0
Strongly disagree	0.00%	0

The 11th question in Round 2 asked the participants for consensus related to the CISO reporting hierarchy developed based on participant responses in Round 1 of the study. The ranking was presented to the participants in this question to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 30 shows the

participants' responses to this question showing that consensus was not reached for question 11 among the panel of experts.

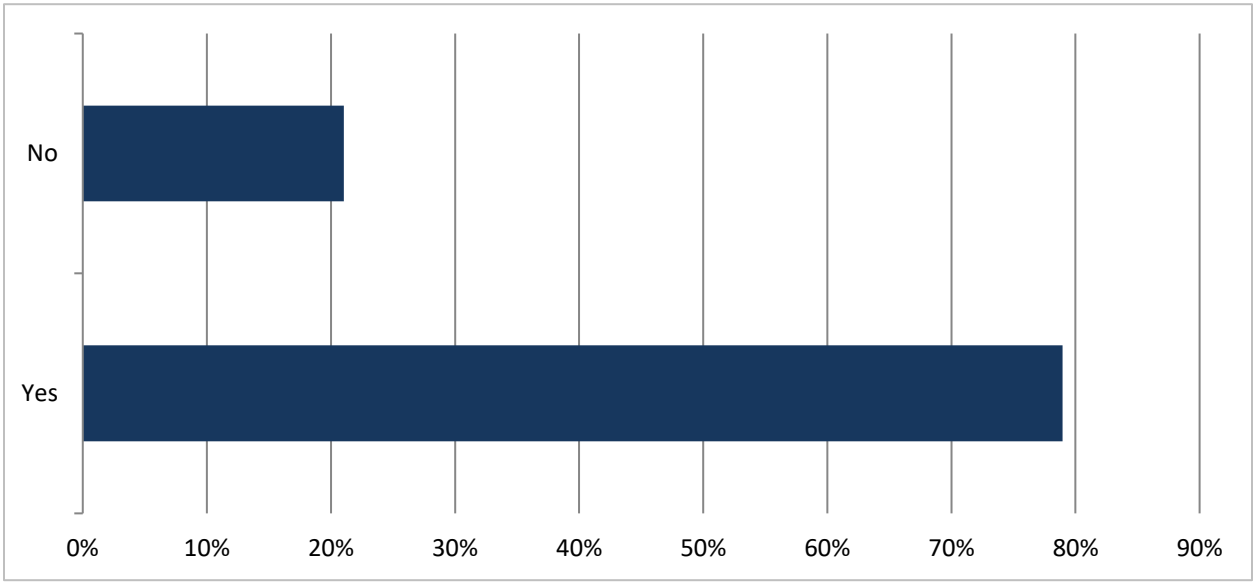

Figure 30. Responses from Question 11 of Round 2

Table 29 provides a summary analysis of the respondent's answers to question eleven. Consensus was not reached related to the CISO reporting hierarchy. The participants provided comments allowing the researcher to improve the question for use in the Round 3 questionnaire. Expert 2 stated that "if the CISO reports to the CIO, it makes cybersecurity an IT function in most cases. It is instead a mission function and should be elevated to a more appropriate level." Expert 13 noted that "CISO reporting should remain in the "C-Suite." The CIO and CISO need to mesh closely to ensure coordination between corporate technology and security.

Table 29

Responses from Question 11 of Round 2

Question Response	Response Percentage	Number of Respondents
Yes	78.95%	15
No	21.05%	4

After analyzing the responses to the twelfth question within Round 2, which was "Is there any additional information you would like to provide related to the role of the CISO that will empower the CISO to succeed within an organization?" the researcher identified themes that were then categorized under organizational culture theory. Figure 31 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question 12 from Round 2, (a) business alignment, (b) organizational change, (c) program management, (d) leadership, and (e) risk management were the top five themes identified by panelists as it related to additional information that the participants wished to convey.

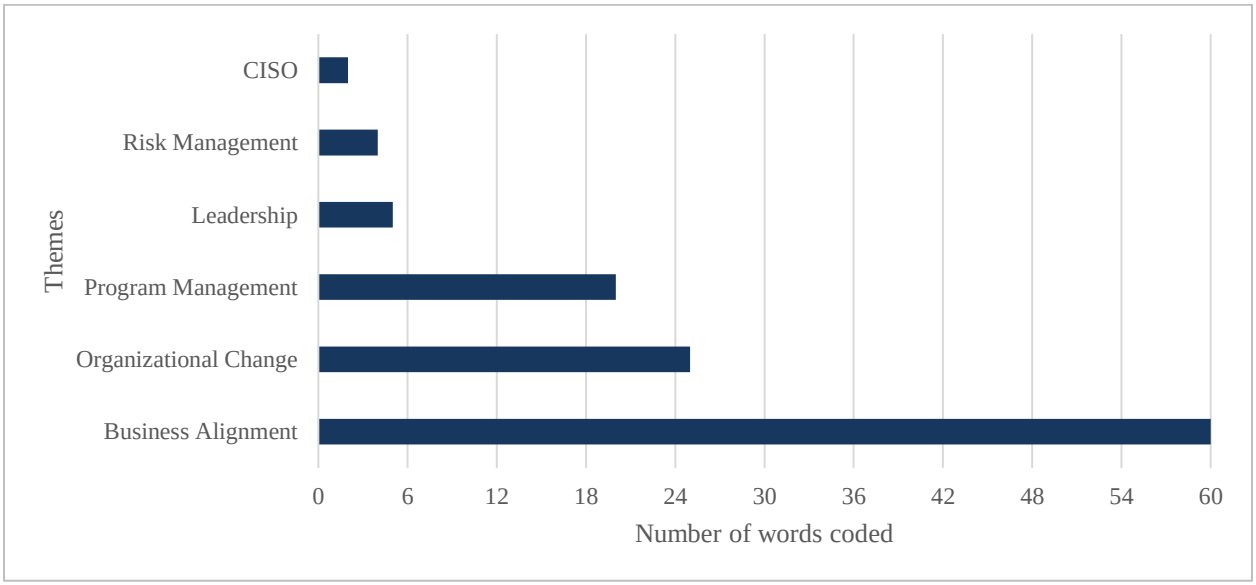

Figure 31. Responses from Question 12 of Round 2

Expert 1 stated that "the CISO is only as effective as those who support the security program. The CISO must be able to influence up, down, and across the organization and leadership structure." Expert 7 noted that "A successful CISO is one that is both confident & knowledgeable in their own right but knows when to ask for help when needed." The themes related to additional information that the participants wished to convey were then categorized against organizational culture theory, as shown in Table 30. The Organizational Culture Theory

level of Assumptions was the top-level identified with 14 total references followed by Beliefs and artifacts, both with two references each. Assumptions contained the greatest score associated with the top five themes identified by panelists related to the topic of security knowledge.

Table 30

Responses from Question 12 of Round 2

Categories	Identified Themes	Number of References
Artifacts	Risk Management	2
Beliefs	Program Management	2
Assumptions	Business Alignment	7
	Organizational Change	3
	CISO	2
	Leadership	2

The data analyzed from Round 2 revealed little consensus amongst the expert panel. Out of the 12 questions asked in Round 2, 8 of the questions yielded no consensus amongst the expert panel. Figure 32 shows the response characteristics of the questions in round 2. Only three questions gained consensus. Eight questions yielded no agreement, and one question was open-ended and designed to provide illuminating information that supported chapter five analysis.

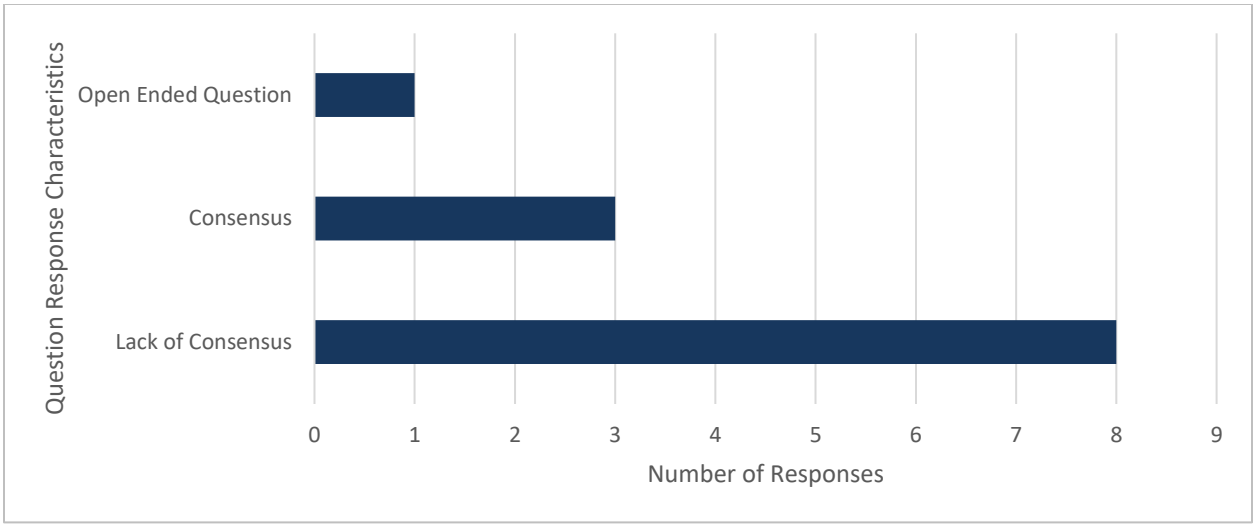

Figure 32. Round 2 Response Characteristics

Table 31 summarizes the response characteristics for the questions in Round 2. The three questions that received consensus in Round 2 was question two, four, and five. Question two asked the participants to review and provide their expert opinion related to a business partner and integrator's definition. Question four asked about security architecture, and question five asked about security program management. As these three questions received consensus in Round 2, they were omitted from the Round 3 survey.

Table 31

Round 2 Response Characteristics

Question Response Characteristics	Number of Questions
Lack of Consensus	8
Consensus	3
Open-Ended Question	1

Once the data analysis concluded for Round 2, the researcher synthesized the participant's information to create the Round 3 questions. Round 3 continues to gain consensus on the role of the CISO. Based on the data provided by the participants and synthesized by the researcher, Round 3 served to achieve consensus on the definition of the roles by the expert panel and the rankings of both the CISO roles and the CISO reporting structure.

Data Analysis Round 3

The data provided by the expert panel in Round 2 provided the information necessary to prepare the Round 3 questionnaire. The Round 3 questionnaire was used to gain final consensus on the definitions related to the role of the CISO. Strong consensus (Smith et al., 2012) was identified for the ranking of roles and the reporting structure of the CISO, but complete consensus was not able to be obtained. Round 3 of the study began on August 26, 2020, and ended on September 08, 2020. The Round 3 questions consisted mostly of closed-ended questions looking for consensus from the panelists related to the content being presented in each question. Microsoft Excel was used to analyze and present the data from all closed-ended questions. For the open-ended questions, a combination of NVivo and Microsoft Excel was used. Thematic analysis was conducted in NVivo. Once the thematic analysis was completed, the data was moved to Excel for editing. The first question in Round 3 asked the participants to determine if they agreed with the ranking presented to them related to the roles needed by the CISO to be successful within a government contracting organization. Table 32 shows the re-ranking of the roles based on participant feedback given in Round 2.

Table 32

ReRanking of Roles Based on Round 2 Feedback

Round 2	Round 3
Risk Management	Risk Management
Governance and Compliance	Strategy and Planning
Security Architecture	Business Partner and Integrator
Strategy and Planning	Governance and Compliance
Security Program Management	Security Knowledge
Technical Security Operations	Security Program Management
Business Partner and Integrator	Communications and Marketing
Security Knowledge	Technical Security Operations
Communications and Marketing	Security Architecture

The new list of roles was presented to the participants to determine if consensus could be reached. If consensus could not be reached, the participant was asked to provide a narrative that would explain what would be needed to make the content acceptable. Figure 33 shows the participants' responses to this question, showing that there is no consensus for question one.

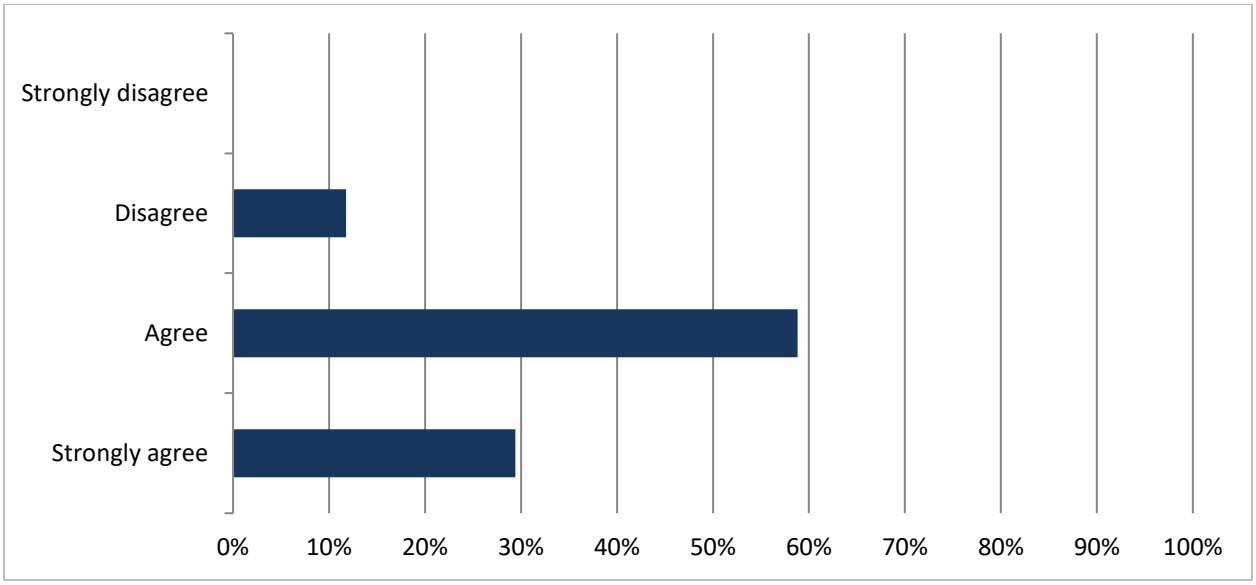

Figure 33. Responses from Question 1 of Round 3

Table 33 provides a summary analysis of the respondent's answers to question one. While complete consensus was not achieved, 88.24% of the respondents, or 15 respondents out of 17, did agree with the ranking showing that strong consensus exists for the CISO role ranking (Smith et al., 2012). An observation made by one of the dissenting panelists was that "Architecture is too low on the list. Like it or not, the CISO position is hardly about strategic goals; it's a highly tactical struggle against mostly acute risk and budgetary negligence."

Table 33

Responses from Question 1 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	29.41%	5
Agree	58.82%	10
Disagree	11.76%	2
Strongly disagree	0.00%	0

In Round 3, the second question asked the participants if they agreed with the definition of technical security operations that was developed based on the expert panels Round 1 and two response. The following is the definition that was provided for the panel's review “The day-to-day operations, maintenance, management, and monitoring of incident response, threat hunting, vulnerability assessment, penetration testing/red teaming, forensics, and disaster recovery services for an organization allowing for risk to be managed to acceptable levels in support of organizational risk management, privacy, and compliance requirements. This capability requires technical depth, leadership, and business/mission alignment to operate and lead security services that focus on operational delivery.”

The definition of technical security operations was presented to the participants to determine if consensus could be reached. Figure 22 shows the participants' responses to this question, showing that consensus was reached for question two amongst the panel of experts.

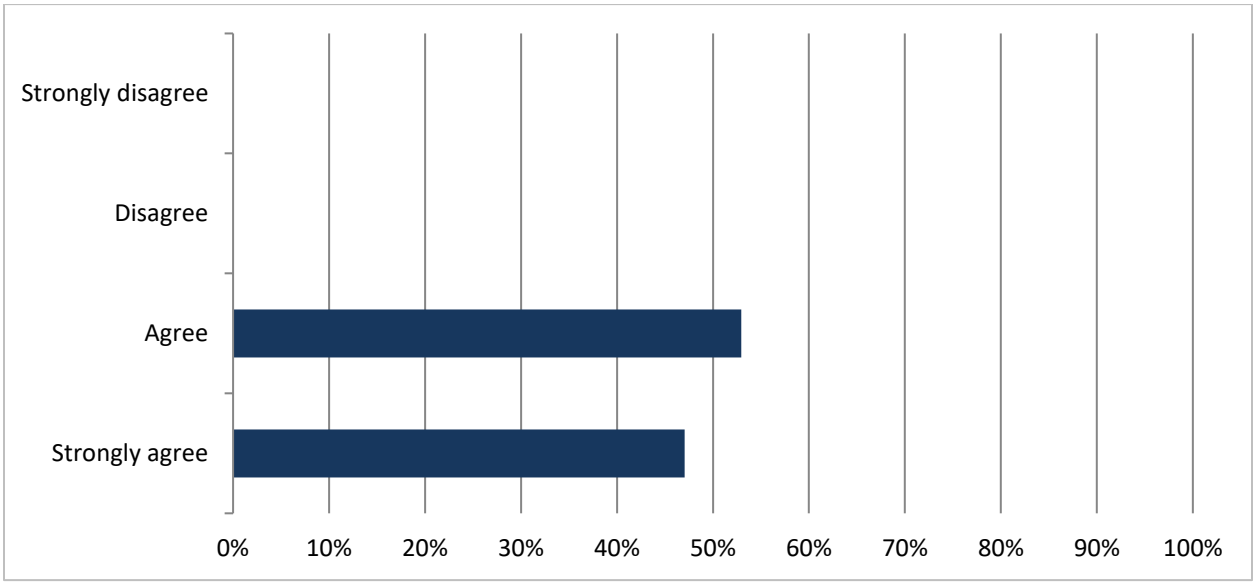

Figure 34. Responses from Question 2 of Round 3

While consensus exists for this question and definition, Expert 1 noted that “technical security operations are the people, tools and processes that identify the vulnerabilities, threats

and activities occurring within the network and direct or execute mitigation of those which will negatively impact information security and cybersecurity." Expert 4 stated, "this is the function focused on what I consider the daily business as usual work that occurs based on established processes and occurs regardless of strategy, business objectives, etc." Table 35 provides a summary analysis of the respondent's answers to question two. All participants agreed with the definition of technical security operations.

Table 34

Responses from Question 2 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	47.06%	8
Agree	52.94%	9
Disagree	0.00%	0
Strongly disagree	0.00%	0

The third question in Round 3 asked the participants if they agreed with the definition of governance and compliance developed based on the expert panels Round 1 and two responses. The following is the definition that was provided for the panel's review "A company's strategy for managing the broad issues of governance, risk management, and corporate compliance with all relevant federal, state, local, and business sector regulatory compliance requirements. This includes ensuring that stakeholder, legal, regulatory, and contractual requirements are evaluated, understood, implemented, and enforced as part of a security program and information system implementation." Figure 35 shows the participants' responses to this question, showing that consensus was reached for question three amongst the panel of experts.

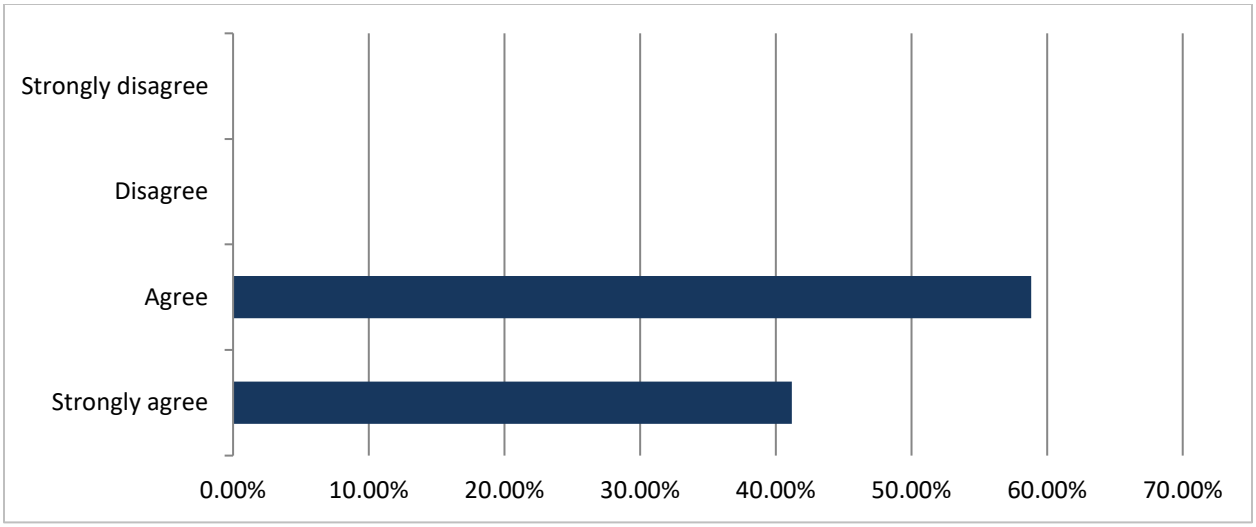

Figure 35. Responses from Question 3 of Round 3

Table 36 provides a summary analysis of the respondent's answers to question three. All participants agreed with the definition of governance and compliance. Consensus exists for this question and definition. Expert 3 explained that "organizationally, governance and compliance is the place where external requirements are consolidated, monitored and reported." Expert 10 noted that "Compliance is literally how many of the security controls in your network meet the framework/guidance in questions- e.g., NIST 800-171 how many controls do you have in place and how many POA&MS are outstanding."

Table 35

Responses from Question 3 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	41.18%	7
Agree	58.82%	10
Disagree	0.00%	0
Strongly disagree	0.00%	0

In Round 3, the fourth question asked the participants if they agreed with the definition of risk management developed based on the expert panels Round 1 and 2 responses. The definition of risk management was presented to the participants in this question to determine if consensus could be reached. Figure 36 shows the participants' responses to this question, showing that agreement was reached for question four amongst the panel of experts.

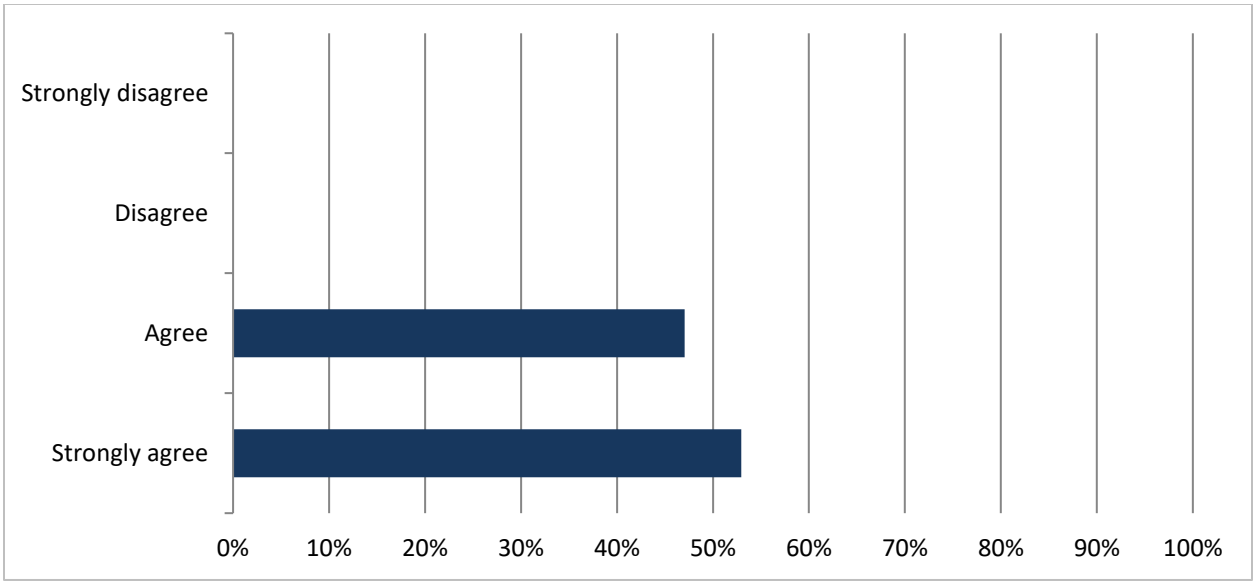

Figure 36. Responses from Question 4 of Round 3

The following is the definition that was provided for the panel's review "Defining, analyzing, and quantifying top cybersecurity risks to revenue, profit, and competitiveness to manage priorities among risks to which funds will be allocated for remediation. This includes developing, operating, and leading while defining, enforcing, and documenting risk - to set and maintain a compliant (and operable) risk posture for the organization. Treatment plans are developed to address risks that are outside of the risk appetite of the organization based on a careful evaluation of threat actors, actor motivation, threats, threat likelihood, vulnerabilities, asset value, asset criticality, and the impact on a system, the organization, or the public. Not all risk can be eliminated from any given environment. The goal of Risk Management is to reduce

risk to an acceptable level where the residual risk can be measured and is in alignment with management expectations."

While consensus exists for this question and definition, Expert 2 stated that "cybersecurity risk management is the measure of risk based on vulnerabilities, the value of information, contextual threats, balanced by countermeasures or controls, and further refined by the likelihood of an incident." Expert 19 explained that "the ability to develop, operate and lead while considering the risk facing an organization mission or systems encapsulates risk management." Table 37 provides a summary analysis of the respondent's answers to question four. All participants agreed with the definition of governance and compliance.

Table 36

Responses from Question 4 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	52.94%	9
Agree	47.06%	8
Disagree	0.00%	0
Strongly disagree	0.00%	0

The fifth question in Round 3 asked the participants if they agreed with the definition of communication and marketing developed based on the expert panels Round 1 response. The following is the definition that was provided for the panel's review "Evangelizing and disbursing information and ideas to establish buy-in at all organizational levels, about the organization's security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis. The ability to communicate with

business stakeholders about the importance and value of security considerations and market the business enabler that a sound security program provides for an organization. Communications and marketing are directed at all levels of the organization to ensure a corporate culture of security is developed and maintained." The definition of communication and marketing was presented to the participants to determine if consensus could be reached. Figure 37 shows the participants' responses to this question, showing that consensus was reached for question five amongst the panel of experts.

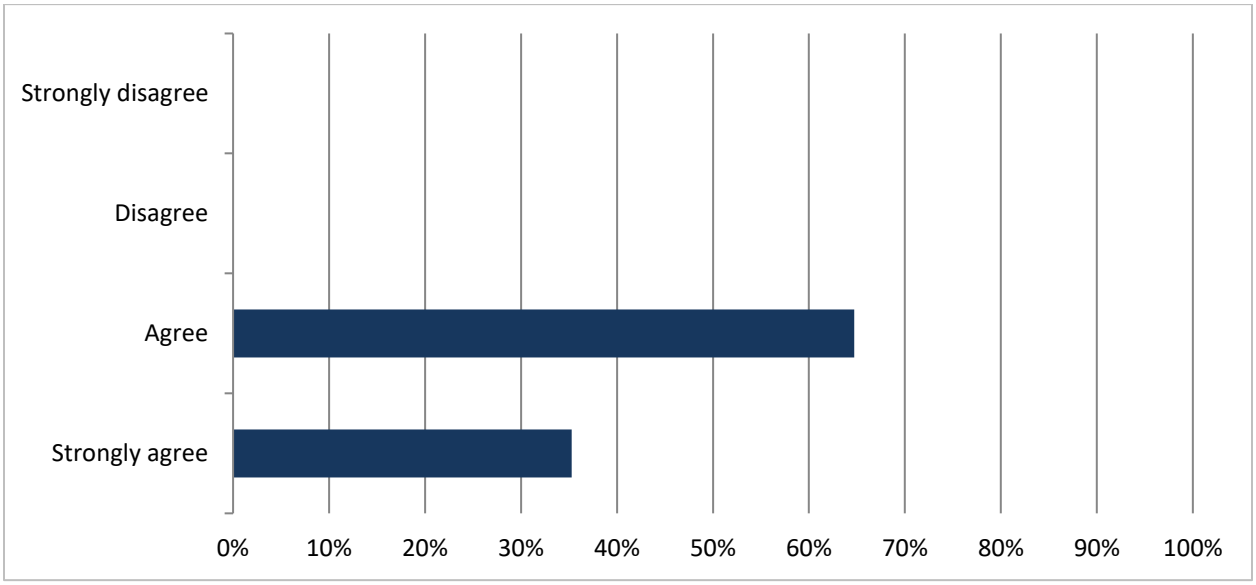

Figure 37. Responses from Question 5 of Round 3

Table 38 provides a summary analysis of the respondent's answers to question five. All participants agreed with the definition of communication and marketing. Consensus exists for this question and definition. Expert 8 explained that "communication and marketing is constantly educating employees on the impact of cyber incidents and explaining what they can do to help protect the customer and company data, as well as why they should." Expert 15 noted that "communications and marketing are essential components of an effective security program. It

impacts buy-in at all organizational levels, as well as budget approval, awareness, ownership, and your sensor 'network' of employees and contractors."

Table 37

Responses from Question 5 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	35.29%	6
Agree	64.71%	11
Disagree	0.00%	0
Strongly disagree	0.00%	0

In Round 3, the sixth question asked the participants if they agreed with the definition of strategy and planning developed based on the expert panels Round 1 and two responses. The following is the definition that was provided for the panel's review "A forward-looking view of the security program's current state, what needs to be accomplished, and the steps necessary to achieve a target state. This is achieved by analyzing the business's needs and the expected evolution of IT within the environment. This leads to the setting of goals and objectives that align the security program with the business's needs, delivering the security program's target state via well-developed security plans easily understood by business leaders. By aligning the security program with corporate goals, a vision and path forward are promoted and integrated with the business's mission."

The definition of strategy and planning was presented to the participants to determine if consensus could be reached. Figure 38 shows the participants' responses to this question, showing that consensus was reached for question six amongst the panel of experts.

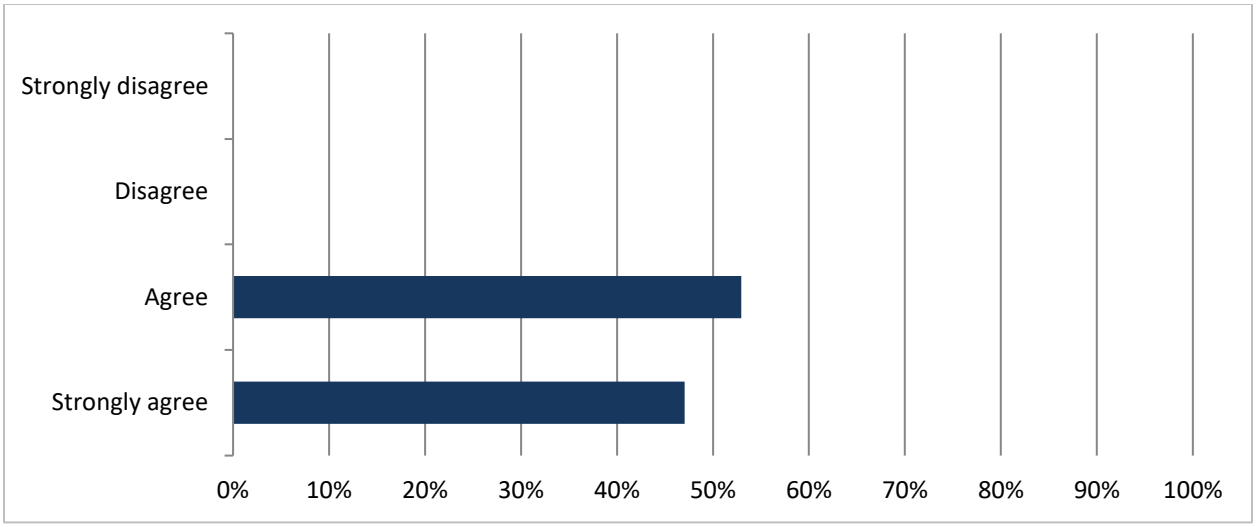

Figure 38. Responses from Question 6 of Round 3

Table 39 provides a summary analysis of the respondent's answers to question six. All participants agreed with the definition of strategy and planning. Consensus exists for this question and definition. Expert 11 stated that "strategy and planning is all about the relationships. Get to know all senior leadership and developing a joint strategy aligning with the business to meet the goals of the organization." Expert 17 noted that "the alignment of high-level corporate goals with the programs and projects intended to accomplish those goals securely" describes strategy and planning.

Table 38

Responses from Question 6 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	47.06%	8
Agree	52.94%	9
Disagree	0.00%	0
Strongly disagree	0.00%	0

In Round 3, the seventh question asked the participants if they agreed with the definition of security knowledge developed based on the expert panels Round 1 and two responses. The following is the definition that was provided for the panel's review "Ability to understand security, privacy, and compliance concerns in full alignments with the business's needs to protect the confidentiality, integrity, and availability of sensitive information and assets factoring in risks and requirements that an organization has concerning security, privacy, and compliance. Having the competencies required to implement a risk-based security program that incorporates the complex, interconnected nature of the enterprise environment and maintains a secure, compliant, operationally effective, and efficient security posture." The definition of security knowledge was presented to the participants to determine if consensus could be reached. Figure 39 shows the participants' responses to this question, showing that consensus was reached for question seven amongst the panel of experts.

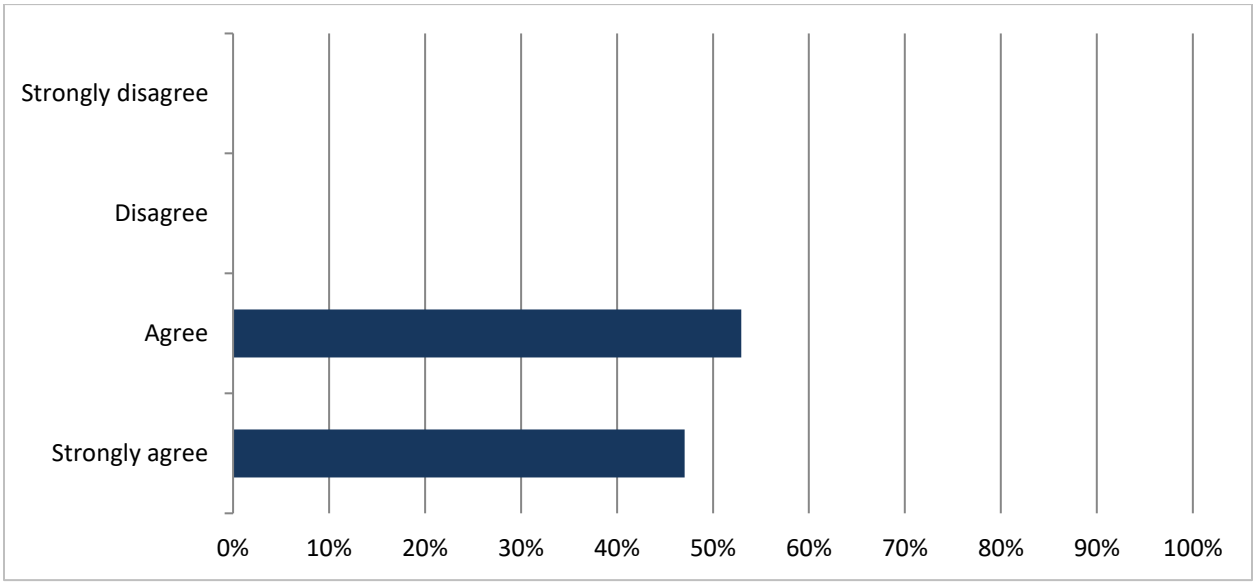

Figure 39. Responses from Question 7 of Round 3

While consensus exists for this question and definition, Expert 14 explained that "security knowledge is an understanding of the risks and requirements an organization has concerning security, privacy and compliance." Expert 15 stated that "security knowledge is an understanding of the various domains of security as well as the ability to apply that knowledge." Table 40 provides a summary analysis of the respondent's answers to question seven. All participants agreed with the definition of security knowledge.

Table 39

Responses from Question 7 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	47.06%	8
Agree	52.94%	9
Disagree	0.00%	0
Strongly disagree	0.00%	0

In Round 3, the eighth question asked the participants for consensus related to the CISO reporting hierarchy developed based on participant responses in Round 1 and two of the study. The ranking was presented to the participants in this question to determine if consensus could be reached. Figure 40 shows the participants' responses to this question showing that consensus was not reached for question eight amongst the panel of experts.

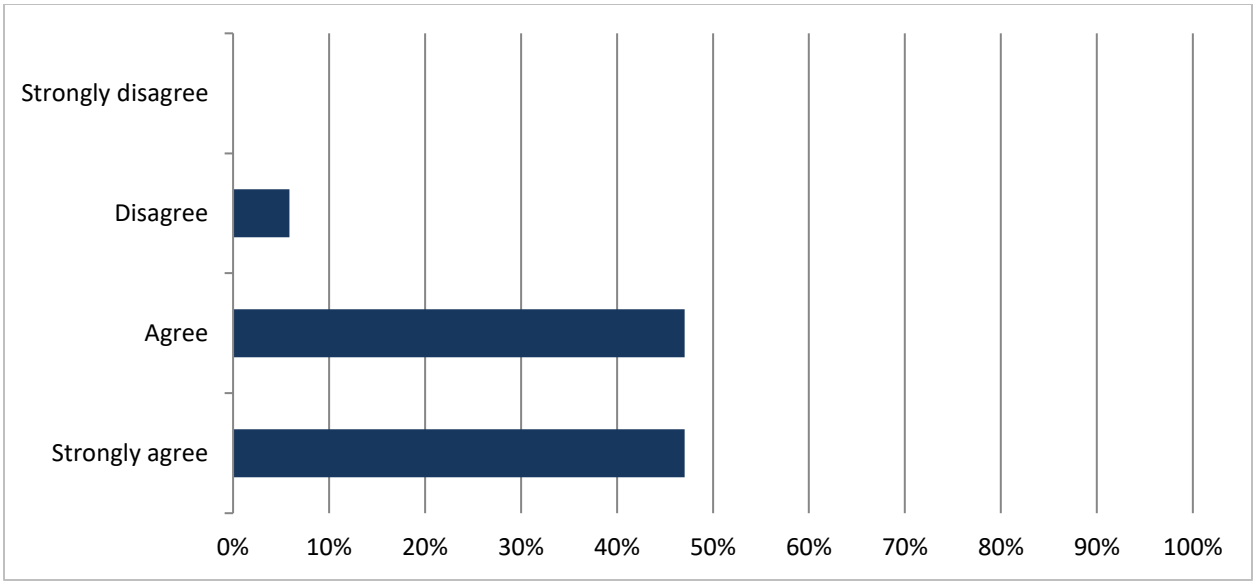

Figure 40. Responses from Question 8 of Round 3

Table 42 provides a summary analysis of the respondent's answers to question eight. While complete consensus was not able to be achieved, 94.12% of the respondents, or 16 respondents out of 17, did agree with the ranking showing that strong consensus exists for the CISO reporting hierarchy (Smith et al., 2012). Expert 1 explained that "I believe the CISO is best served by an organizational chain of responsibility that includes the CIO, CTO and CFO and easy access to the CEO and Board. This ensures the CISO has equal and unfettered access and influence to the key decision-makers and who can bring the CISO's perspectives and approaches to the rest of the business leaders." Expert 10 noted that "The CIO operates the network and provides a service to the company using IT to meet business objectives. The CIO needs to provide a secure IT service. A CISO focuses on security and can inform the CIO of risk and supports the CIO in defining a security architecture, budget and policies."

Table 40

Responses from Question 8 of Round 3

Question Response	Response Percentage	Number of Respondents
Strongly agree	47.06%	8
Agree	47.06%	8
Disagree	5.88%	1
Strongly disagree	0.00%	0

After analyzing the responses to the ninth question within Round 3, which was "Is there any additional information you would like to provide related to the role of the CISO that will empower the CISO to succeed within an organization?" the researcher identified themes that were then categorized under organizational culture theory. Expert 15 stated that "CISOs often focus on compliance as an initial (and sometimes final) step. Striving for compliance can lead to a checkbox exercise where the program falls short of implementing effective security. CISOs should certainly ensure legal, regulatory, and contractual measures are met but the goal should be a system that is understood, actively monitored, and is resilient." Expert 19 stated that "the soft skills such as communication, collaboration and vision should be considered in partnership with security experience and technical proficiency as they combine for a well-rounded security executive." Figure 41 provides the analysis of the coded themes and word count for each theme. Based on the analysis of question nine from Round 3, (a) program management, (b) risk management, (c) business alignment, (d) organizational change, and (e) training and education were the top five themes identified by panelists as it related to additional information that the

participants wished to convey.

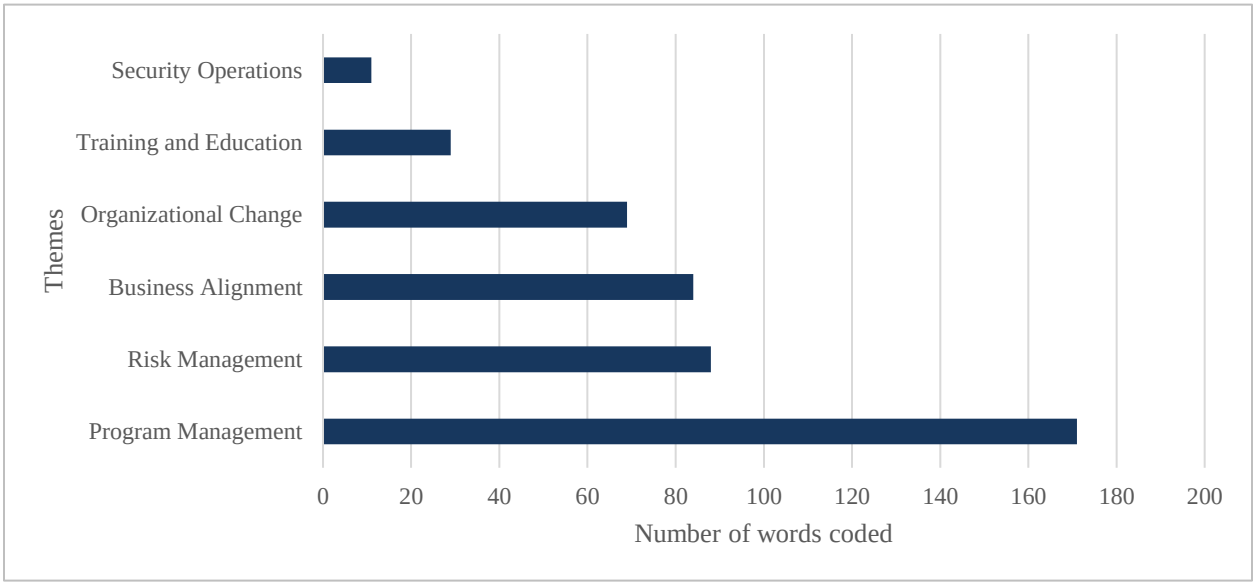

Figure 41. Themes from Question 9 of Round 3

The themes related to additional information that the participants wished to convey were then categorized against organizational culture theory, as shown in Table 43. The Organizational Culture Theory level of Assumptions was the top-level identified with 12 total references, followed by Beliefs with eight references and, finally, artifacts with six references. Assumptions contained the greatest score associated with the top five themes identified by panelists related to the topic of security knowledge.

Table 41

Themes from Question 9 of Round 3

Categories	Identified Themes	Number of References
Artifacts	Risk Management	5
	Security Operations	1
Beliefs	Program Management	8

Categories	Identified Themes	Number of References
Assumptions	Business Alignment	5
	Organizational Change	4
	Training and Education	3

The data analyzed from Round 3 revealed complete consensus across most questions amongst the expert panel. Out of the nine questions asked in Round 3, 6 of the questions yielded complete consensus amongst the expert panel. Figure 42 shows the response characteristics of the questions in round 3, where six questions gained consensus, two questions yielded no consensus, and one question was open-ended and designed to provide illuminating information that supported chapter five analysis.

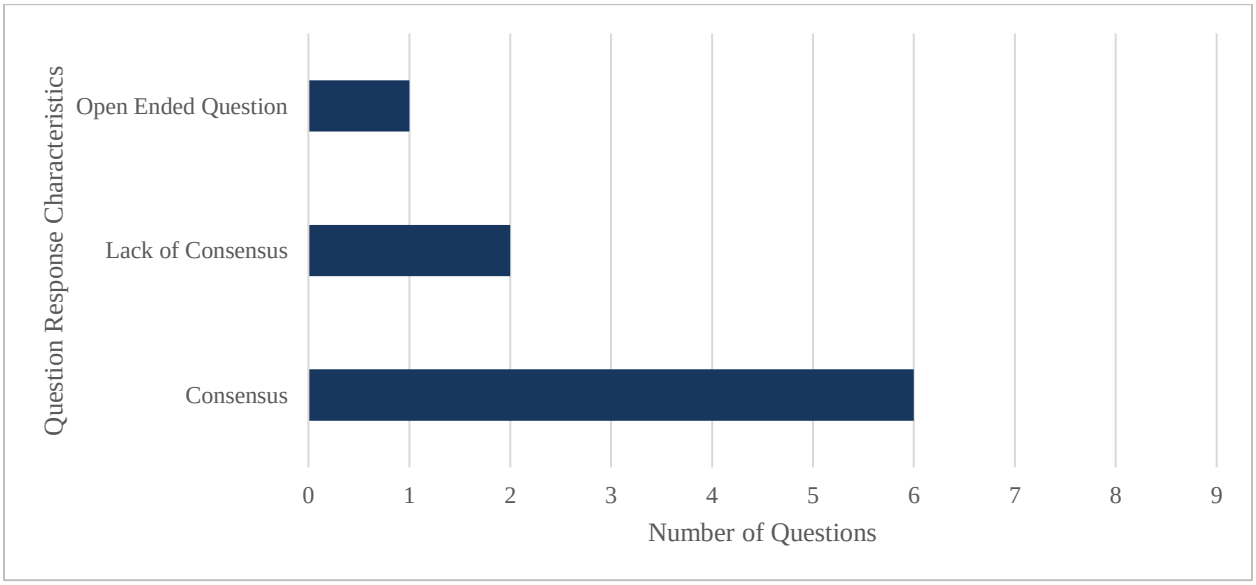

Figure 42. Round 3 Response Characteristics

Table 42 summarizes the response characteristics for the questions in Round 3. All definition questions received complete consensus from the expert panel in Round 3. The two ranking questions did obtain strong consensus amongst the expert panel (Smith et al., 2012).

Table 42

Round 3 Response Characteristics

Question Response Characteristics	Number of Questions
Lack of Consensus	2
Consensus	6
Open-Ended Question	1

The data analyzed from Round 1, Round 2, and Round 3 revealed common themes across the study. Figure 43 shows the top five themes identified across all of the open-ended questions in the study.

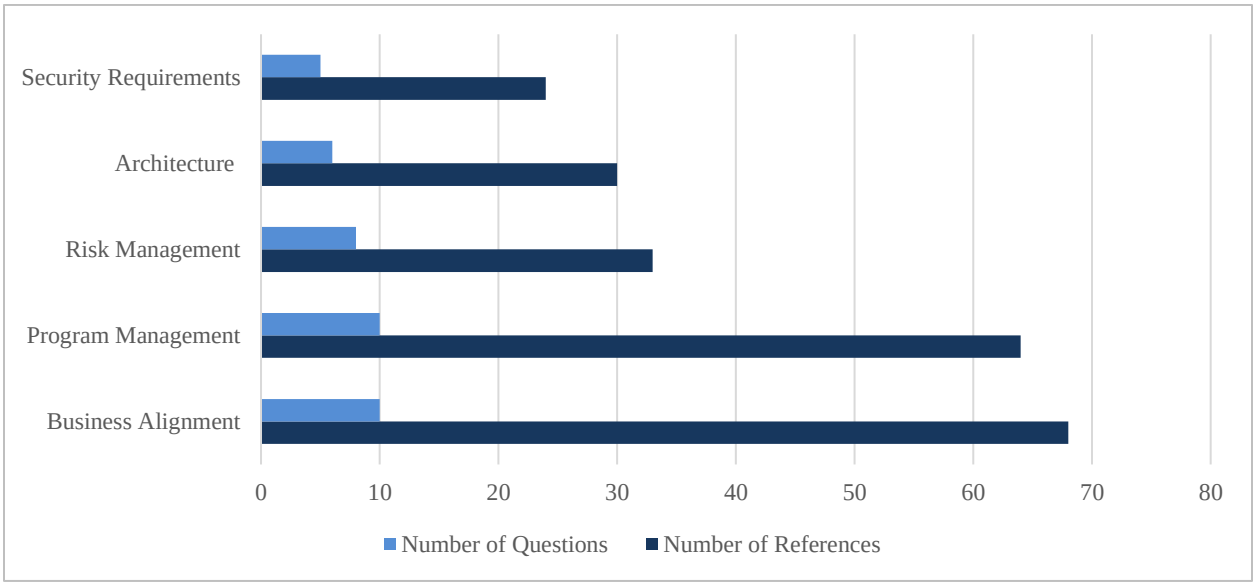

Figure 43. Top Five Themes Identified Across Study

The top five themes identified across all of the open-ended questions in the study are (a) business alignment, (b) program management, (c) architecture, (d) risk management, and (e) security requirements. These top five themes were identified in Round 1 and remained the top five themes for the study. Additional data collected throughout the study support the top themes

initially identified in Round 1. Table 43 summarizes the top themes identified across the study showing the number of references for each theme and the number of times that a theme is present within a question.

Table 43

Top Five Themes Identified Across Study

Themes	Number of References	Number of Questions
Business Alignment	68	10
Program Management	64	10
Risk Management	33	8
Architecture	30	6
Security Requirements	24	5

Figure 44 shows the distribution of themes across the levels of Organizational Culture Theory. Assumptions were the most often identified level with 186 references. Artifacts were the second most used level, with 176 references. Finally, Beliefs was the least categorized level with 154 references.

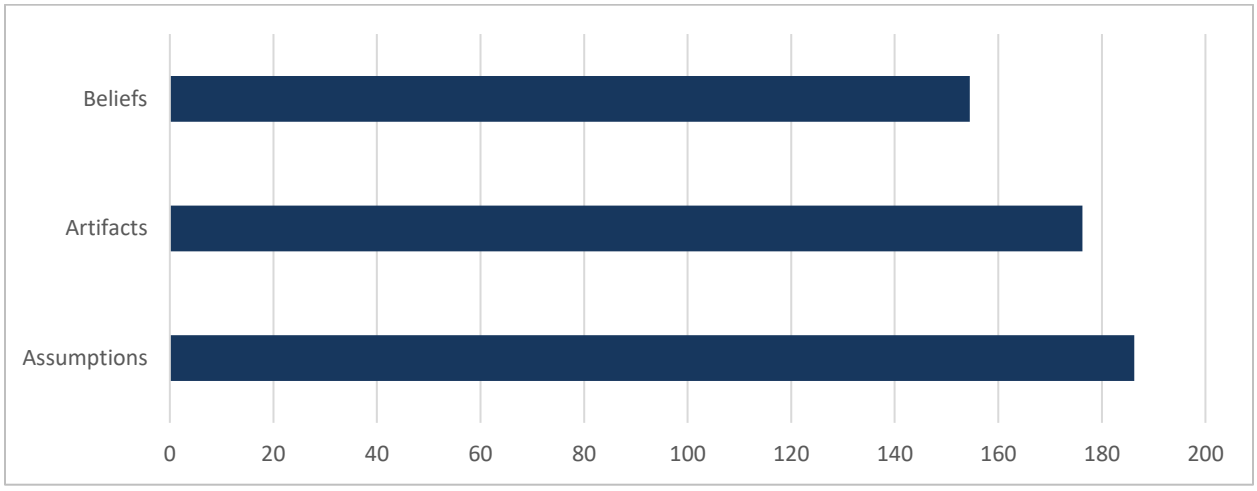

Figure 44. Organizational Culture Theory Summary for Study

Table 44 summarizes the distribution of theme references across the levels of Organizational Culture Theory that are present throughout the study. While the top themes that were identified did not change, the distribution of organizational culture theory levels changed from Round 1 to the end of the study. Table 44 shows that in Round 1, Artifacts was the most often references OCT level. However, by the end of the study, Assumptions was the most referenced level. Assumptions and Artifacts flipped position while Beliefs remained the least reverenced Organizational Culture theory level.

Table 44

Organizational Culture Theory Summary for Study

Levels	Number of References Round 1	Number of References Entire Study
Assumptions	164	186
Artifacts	167	176
Beliefs	139	154

Member Checking

During the member checking phase of this study, Expert 1 noted that "The CISO is only as powerful and effective as those who support the security program. The CISO must be able to influence up, down, and across the organization and leadership structure." Expert 10 expanded on the concept of leadership alignment with a discussion of the security program budget. Expert 10 added that "a CISO must have a budget and funds available that move with the threat landscape. The funding should always be available rather than a mad scramble to obtain funds to address resiliency shortcomings in the organization." Expert 9 also mentioned that "as a leader, the CISO ensures that the security program is adding value across the business. Additionally, the CISO outlines the cyber risk to the business and how the cybersecurity program can mitigate that

risk for the company. The CISO also supports any strategic and digital transformation initiatives established by the corporation." The CISO builds support with an organization's executive leadership to implement a successful cybersecurity strategy to ensure a resilient and robust company (Ogutu et al., 2018).

Additional insights were brought up by Expert 4 related to the role of the CISO as it relates to business alignment and developing technical architectures that serve to align with the organization's value chain. Expert 4 explained that "architecture as it relates to the overall organizational environment, its policies, standards, and requirements has the opportunity to be embedded in more extensive technical efforts to ensure that security standards are being followed to reduce business risk." Expert 11 highlighted the need for an overall practical approach to cybersecurity program management that included the right people, processes, and tools to secure and support the business's needs. Expert 11 explained that a "well-managed security program includes developing a strategy and implementation plan to instantiate information security and cybersecurity services for the business. This approach includes supporting a cost-effective set of tools, motivating and supporting the right mix of services, people, and skills to implement and manage those tools, processes, and procedures to ensure that security is established and audited. Finally, all program components must be adequate, current, and managed within a security framework and security life cycle."

The examples discussed by these experts are fully aligned and support the identified themes of this study, which are (a) Business Alignment, (b) Program Management, (c) Risk Management, (d) Architecture, and (e) Security Requirements. Additionally, the examples discussed by these experts are aligned with prior research on information technology and information security leadership. For example, The CISO must ensure that the information

security program enables mission and business objectives and adds value to mission capabilities (Rothrock et al., 2018). Cybersecurity should be strategically aligned with the business's mission and viewed as a business enabler. Based on the expert panel's information, the researcher developed a proficient response to the research question under examination.

> RQ: To what extent is there a consensus among a panel of security experts as to the roles of the CISO as it relates to establishing and maintaining a government contracting organization's information and data security?

Table 45 provides the ranked order of CISO skills required by the government contracting CISO to be successful in their role. The ranking of importance is 1 through 9, with 1 being the most critical and 9 being the least important role.

Table 45

CISO Roles Ranked by Importance

Rank Order	CISO Roles Ranked by Importance
1	Risk Management
2	Strategy and Planning
3	Business Partner and Integrator
4	Governance and Compliance
5	Security Knowledge
6	Security Program Management
7	Communications and Marketing
8	Technical Security Operations
9	Security Architecture

To accompany the rankings, it was essential to understand the expert panel's definition of each ranking. The following section provides the definitions for each role developed based on the panelists' feedback.

Risk Management - Defining, analyzing, and quantifying top cybersecurity risks to revenue, profit, and competitiveness to manage priorities among risks to which funds will be allocated for remediation. This includes developing, operating, and leading while defining, enforcing, and documenting risk - to set and maintain a compliant (and operable) risk posture for the organization. Treatment plans are developed to address risks that are outside of the risk appetite of the organization based on a careful evaluation of threat actors, actor motivation, threats, threat likelihood, vulnerabilities, asset value, asset criticality, and the impact on a system, the organization, or the public. Not all risk can be eliminated from any given environment. The goal of Risk Management is to reduce risk to an acceptable level where the residual risk can be measured and is in alignment with management expectations.

Strategy and Planning – A forward-looking view of the security program's current state, what needs to be accomplished, and the steps necessary to achieve a target state. This is achieved by analyzing the business's needs and the expected evolution of IT within the environment. This leads to the setting of goals and objectives that align the security program with the business's needs, delivering the security program's target state via well-developed security plans easily understood by business leaders. By aligning the security program with corporate goals, a vision and path forward are promoted and integrated with the business's mission.

Business Partner and Integrator - Someone that understands business priorities and challenges so that security is an enabler. They can communicate and partner with members of the business to achieve objectives securely and safely aligned with organizational risk appetite. Business

partners and integrators help to address gaps and augment organizational capabilities participating in discussions related to the connection of systems and the flow of business data bringing oversight, monitoring, and secure implementation capabilities to an engagement.

Governance and Compliance - A company's strategy for managing the broad issues of governance, risk management, and corporate compliance with all relevant federal, state, local, and business sector regulatory compliance requirements. This includes ensuring that stakeholder, legal, regulatory, and contractual requirements are evaluated, understood, implemented, and enforced as part of a security program and information system implementation.

Security Knowledge - Ability to understand security, privacy, and compliance concerns in full alignments with the business's needs to protect the confidentiality, integrity, and availability of sensitive information and assets factoring in risks and requirements that an organization has concerning security, privacy, and compliance. Having the competencies required to implement a risk-based security program that incorporates the complex, interconnected nature of the enterprise environment and maintains a secure, compliant, operationally effective, and efficient security posture

Security Program Management – The leadership (regular, active management) of a program which provides operational roadmaps, security resources, and standards for an organization, in addition to operational capabilities that ensure the selection and implementation of management, operational, and technical security controls commensurate with both the risk and regulatory requirements of the enterprise. Security program management also encompasses the projects, programs, and portfolio management of security-related initiatives that support compliance, risk management, POAM resolution, technology development, policies/procedures, training, and funding which are coordinated to produce a resilient organization.

Communications and Marketing - Evangelizing and disbursing information and ideas to establish buy-in at all organizational levels, about the organization's security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis. The ability to communicate with business stakeholders about the importance and value of security considerations and market the business enabler that a sound security program provides for an organization. Communications and marketing are directed at all levels of the organization to ensure a corporate culture of security is developed and maintained.

Technical Security Operations - Technical security operations are the day-to-day operations, maintenance, management, and monitoring of incident response, threat hunting, vulnerability assessment, penetration testing/red teaming, forensics, and disaster recovery services for an organization allowing for risk to be managed to acceptable levels in support of organizational risk management, privacy, and compliance requirements. This capability requires technical depth, leadership, and business/mission alignment to operate and lead security services that focus on operational delivery.

Security Architecture - Ability to define a framework and plan to implement an architecture and corporate security culture which decreases operational risk, enhances organizational security, and provides security standards for an organization's digital systems and components to address security, privacy, and compliance concerns. Security architecture requires one to think broadly about the interplay of various technology pieces as they develop technical blueprints, which allow for secure solution implementation supporting continuous security monitoring.

Finally, the last piece of data gathered and analyzed that supports the role of the CISO within the government contracting organization is the CISO reporting structure. The ranking of

importance is 1 through 2, with 1 being the most crucial and 2 being the least desirable reporting structure.

Table 46

CISO Reporting Structure

Rank Order	CISO Reporting Structure
1	CEO
2	CIO

Summary

Chapter 4 included a review of the problem and research question under investigation and the rationale behind why this study is essential to support the U.S. federal government contractor in meeting new and change cybersecurity requirements. The tools used to conduct the research were discussed, which included tools for data collection and data analysis/presentation. The mechanisms used to recruit the study sample, in addition to the location used for recruitment, were discussed. The inclusion criteria that were used to determine the expert status for a panel member was discussed. The process used to shift from recruitment to study execution was discussed, including how communications were handles with study participants. The number of participants and how these panelists stayed active throughout the study was discussed. Finally, the expert developed skill ranking, CISO reporting hierarchy, and role definitions were included at the end of this chapter to answer the research question under examination.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Introduction

The role of chief information security officer and the skills needed to perform the function of information security management leadership for an organization need to be well understood due to the essential functions provided by the CISO in support of organizational resiliency and security (Haqaf, & Koyuncu, 2018). The role of the CISO and technology leadership in protecting mission execution, identifying risk, and supporting mission success has become critical in ensuring organizational resiliency (Griffy-Brown et al., 2019). As digital systems have proliferated across government contractor enterprises, the need to protect sensitive governmental information on government contracting systems has become a priority (Doubleday, 2019). For the government contracting organization, the need to safeguard governmental and sensitive information has further projected the need for a close relationship between the business units of the organization and the CISO (Trope, 2018). As the CISO works to develop the organization's information security program in partnership with the business leadership, critical aspects of the organization will be addressed related to how technology is used and how data is protected within the organization.

As government requirements have begun to mature related to supplier security, it is apparent that the government is starting to take the technical controls implemented by its suppliers much more seriously (Bak, 2018). The suppliers to the U.S. federal government offer a vector of attack onto a government agency’s enterprise network or access to sensitive government data that may reside on the contractor’s network (Gunzel, 2017). Due to the risk inherent in the supplier/customer relationship between contractors and federal agencies, the U.S. federal government has developed and promulgated standards to ensure sensitive governmental

information residing on government contractor digital systems are safeguarded (Ross et al. 2018). Measures like these are designed to motivate the government contractor community to make more secure choices related to their implementation of information systems that support U.S. federal contracts (Reagin, & Gentry, 2018).

Information technology plays a pivotal role in mission execution for an organization due to the value that technology delivers related to mission delivery (Mithas & Rust, 2016). Because of the great value that information technology brings to the organization, its proliferation has increased at an ever-increasing rate (Griffy-Brown, et al., 2019). Due to this proliferation of digital systems across government contractor enterprises and the need to protect sensitive governmental information on those systems (Trope, 2018), the U.S. federal government has begun to deploy standards designed to safeguard confidential government information on contractor digital systems. These standards provide motivation and guidance for organizations to follow when implementing security controls throughout their organization's enterprise (Reagin, 2018). The CISO is responsible for ensuring that corporate systems meet the federal requirements and that these requirements are met securely.

An exhaustive review of the literature was conducted in chapter two of this study to support the need for research into the roles of the CISO as it relates to establishing and maintaining a government contracting organization's information and data security. While there has been a significant focus on the CISO role from a popular and trade article perspective, a gap was identified related to academic research on the topic of the CISO (Karanja & Rosso, 2017). As limited academic research exists on the subject of the CISO, and no academic research exists related to the CISO for government contracting organizations, this provides an excellent opportunity to provide meaningful research and analysis to further the overall body of

knowledge related to information technology management. Chapter five presents the findings and themes gathered during chapter four and compares them against the existing literature in chapter two. This analysis provides recommendations to support the decision making for government contractors related to internal security protection and the U.S. federal government related to supplier security.

Evaluation of Research Questions

RQ: To what extent is there a consensus among a panel of security experts as to the roles of the CISO as it relates to establishing and maintaining a government contracting organization's information and data security?

To answer the research question, it became necessary to analyze the literature to identify the roles filled by CISOs. This list of roles could then be reviewed by a panel of experts that support government contracting organizations for applicability within their specific industry (Maynard, Onibere, & Ahmad, 2018).

The data analyzed from the Delphi rounds revealed common themes based on the participant's responses. The top five themes identified across all rounds of the study are (a) business alignment, (b) program management, (c) architecture, (d) risk management, and (e) security requirements. These top five themes were identified in Round 1 and remained the top five themes for the study. The identified themes and the expert panel's narrative responses were used to develop the definitions for the roles that are needed by the government contracting CISO. Table 47 shows the top five themes identified from the responses of the participants.

Table 47

Top Five Themes Identified Across Study

Ranking Order	Themes
1	Business Alignment
2	Program Management
3	Risk Management
4	Architecture
5	Security Requirements

Business Alignment

Business alignment was identified as the top theme that was discussed by the expert panel throughout the study. Figure 45 provides a visual representation of the expert panel responses that were categorized related to business alignment.

Figure 45. Business Alignment Word Cloud

Business integration and environmental understanding were identified as a key theme as part of the literature review in chapter two and aligns with the panelists' business alignment theme. A clear connection was made throughout the literature related to the CISOs role and the

importance of business alignment when developing and implementing an information security program (Alexander & Cummings, 2016). Cybersecurity should be viewed as a business enabler and should be strategically aligned with the business's mission. The CISO must work to be an enabler of the mission to ensure that the information security program enables business objectives and adds value to business capabilities (Rothrock et al., 2018).

Program Management

The second theme identified from the expert panel's comments was program management. Figure 46 provides a visual representation of the expert panel responses that were categorized related to program management.

Figure 46. Program Management Word Cloud

The contractor CISO's role in the area of U.S. federal government compliance is vital to the successful implementation of cybersecurity practices within the contracting organization. Throughout the literature review, program management was identified as a critical competency of the CISO and necessary when establishing and managing an enterprise cybersecurity program. The CISO, as the leader of an organization’s security program, is responsible for establishing a mission-focused and robust information security and risk management program for an organization (Murphy, 2018). The CISO works with other executives to build support for

implementing a security program to establish a secure and resilient company (Ogutu et al., 2018).

Risk Management

The third theme identified from the expert panel's comments was risk management. Figure 47 provides a visual representation of the expert panel responses that were categorized related to risk management.

Figure 47. Risk Management Word Cloud

As part of the literature review in chapter two, risk management was covered extensively. The CISO is the key leader responsible for identifying and managing cybersecurity risk for the organization. An organization's ability to operate its mission can be seriously impacted by the organization's security risks (Ogutu et al., 2018). Risk management must be considered from a strategic perspective amongst organizational leadership to establish a resilient and enduring organization (Steinbart, et al., 2018). A practical approach to enterprise risk management is needed to ensure that organizations can effectively identify, document, triage, and mitigate risks that may impact the organization (Ogutu, Bennett, & Olawoyin, 2018).

Architecture

The fourth theme identified from the expert panel's comments was architecture. Figure 48 provides a visual representation of the expert panel responses that were categorized related to architecture.

Figure 48. Architecture Word Cloud

Security architecture capabilities provided by the CISO support the organization's development and implementation of digital technologies. This architecture focus extends beyond development and implementation and into an information system's ongoing operations through one-on-one consultations with technical teams and organizational business units (Hooper & McKissack, 2016). It is essential to understand that security architecture is not only associated with technology but also operational and management competencies (Karanja, 2017). In support of solving technical security problems, the CISO develops secure solutions to business problems and assists with developing alternatives when a selected business technical solution poses a risk to the organization (Death, 2017).

Security Requirements

The fifth theme identified from the expert panel's comments was security requirements. Figure 49 provides a visual representation of the expert panel responses that were categorized related to Architecture.

Figure 49. Security Requirements Word Cloud

Security requirements were covered extensively in the literature review as the CISO is responsible for ensuring that security requirements are developed and integrated into digital systems in accordance with organizational and regulatory requirements. The CISO should be brought into any new technology project discussion as early as possible by being integrated into the organization's Systems Development / Engineering Life Cycle (SDLC / SELC) (Kulkarni, 2018). The earliest stage in a typical SDLC/SELC process is project initiation (Death, 2017). As the business customer proposes new technical capabilities, the project team works to develop the technological solution's functional requirements. During this stage, the CISO should inject security requirements into the project and advise mission leaders related to protecting mission operations.

CISO Roles Ranking and Definitions

The roles of the CISO, ranking, and definition directly support answering the research question under investigation. In conjunction with the identified themes, the responses by the expert panel served to support the creation of the below definitions that were reviewed and received complete consensus from the expert panel. Table 48 provides the roles that are critical for the government contracting CISO. Additionally, the roles included in table 48 are ranked related to importance, with a ranking of 1 being the most important and nine being the least important. Finally, The definition provided for each role was developed based on the responses given by the expert panel, which serves to ensure that future readers can understand what the expert panel understood the roles to be when they ranked them.

Table 48

CISO Roles Ranking and Definitions

Ranking	CISO Roles	Definition
1	Risk Management	Defining, analyzing, and quantifying top cybersecurity risks to revenue, profit, and competitiveness to manage priorities among risks to which funds will be allocated for remediation. This includes developing, operating, and leading while defining, enforcing, and documenting risk - to set and maintain a compliant (and operable) risk posture for the organization. Treatment plans are developed to address risks that are outside of the risk appetite of the organization based

Ranking	CISO Roles	Definition
		on a careful evaluation of threat actors, actor motivation, threats, threat likelihood, vulnerabilities, asset value, asset criticality, and the impact on a system, the organization, or the public. Not all risk can be eliminated from any given environment. The goal of Risk Management is to reduce risk to an acceptable level where the residual risk can be measured and is in alignment with management expectations.
	Strategy and Planning	A forward-looking view of the security program's current state, what needs to be accomplished, and the steps necessary to achieve a target state. This is achieved by analyzing the business's needs and the expected evolution of IT within the environment. This leads to the setting of goals and objectives that align the security program with the business's needs, delivering the security program's target state via well-developed security plans easily understood by business leaders. By aligning the security program with corporate goals, a vision and path forward are promoted and integrated with the business's mission.

Ranking	CISO Roles	Definition
3	Business Partner and Integrator	Someone that understands business priorities and challenges so that security is an enabler. They can communicate and partner with members of the business to achieve objectives securely and safely aligned with organizational risk appetite. Business partners and integrators help to address gaps and augment organizational capabilities participating in discussions related to the connection of systems and the flow of business data bringing oversight, monitoring, and secure implementation capabilities to an engagement.
4	Governance and Compliance	A company's strategy for managing the broad issues of governance, risk management, and corporate compliance with all relevant federal, state, local, and business sector regulatory compliance requirements. This includes ensuring that stakeholder, legal, regulatory, and contractual requirements are evaluated, understood, implemented, and enforced as part of a security program and information system implementation.
5	Security Knowledge	Ability to understand security, privacy, and compliance concerns in full alignments with the business's needs

Ranking	CISO Roles	Definition
		to protect the confidentiality, integrity, and availability of sensitive information and assets factoring in risks and requirements that an organization has concerning security, privacy, and compliance. Having the competencies required to implement a risk-based security program that incorporates the complex, interconnected nature of the enterprise environment and maintains a secure, compliant, operationally effective, and efficient security posture
6	Security Program Management	The leadership (regular, active management) of a program which provides operational roadmaps, security resources, and standards for an organization, in addition to operational capabilities that ensure the selection and implementation of management, operational, and technical security controls commensurate with both the risk and regulatory requirements of the enterprise. Security program management also encompasses the projects, programs, and portfolio management of security-related initiatives that support compliance, risk management, POAM resolution, technology development,

Ranking	CISO Roles	Definition
		policies/procedures, training, and funding which are coordinated to produce a resilient organization.
7	Communications and Marketing	Evangelizing and disbursing information and ideas to establish buy-in at all organizational levels, about the organization's security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis. The ability to communicate with business stakeholders about the importance and value of security considerations and market the business enabler that a sound security program provides for an organization. Communications and marketing are directed at all levels of the organization to ensure a corporate culture of security is developed and maintained.
8	Technical Security Operations	The day-to-day operations, maintenance, management, and monitoring of incident response, threat hunting, vulnerability assessment, penetration testing/red teaming, forensics, and disaster recovery services for an organization allowing for risk to be managed to acceptable levels in support of organizational risk

Ranking	CISO Roles	Definition
		management, privacy, and compliance requirements. This capability requires technical depth, leadership, and business/mission alignment to operate and lead security services that focus on operational delivery.
9	Security Architecture	Ability to define a framework and plan to implement an architecture and corporate security culture which decreases operational risk, enhances organizational security, and provides security standards for an organization's digital systems and components to address security, privacy, and compliance concerns. Security architecture requires one to think broadly about the interplay of various technology pieces as they develop technical blueprints, which allow for secure solution implementation supporting continuous security monitoring.

CISO Reporting Relationship

The final area developed to answer the research question was the reporting structure that would best support the CISO in supporting the business security posture. Table 48 provides the optimal managerial reporting relationship for the CISO as Identified by the expert panel.

Table 49

CISO Reporting Structure

Rank Order	CISO Reporting Structure
1	CEO
2	CIO

One of the respondents' key observations had to do with the CISO reporting to the CIO. This reporting relationship can be extremely healthy when the CIO sees security as a foundational requirement for digital implementations and is a cybersecurity champion. Additionally, it was observed that the CIO must report to the CEO for this relationship to work. “In a case where the CIO reports to a director, that reports to a vice president, that reports to an executive vice president, that reports to the CEO, you should expect the needs of IT and the needs of cybersecurity to be lost in the noise.” In a case where the CIO champions cybersecurity and reports to the CEO, the CISO can safely report the CIO. An organization needs to determine if the relationship is healthy and if reporting accuracy is occurring from the CISO that reports to the CIO. Outside of this observation, the expert panel recommends that the CISO report to the CEO.

Fulfillment of Research Purpose

The fulfillment of the research purpose resulted in understanding the roles and the definition of those roles for the government contracting CISO. Additionally, an understanding of the CISO and their manager's optimal reporting relationship within a government contracting organization. This research is entirely new within the government contracting industry, as no investigation of this type has been performed before this study. The literature review of this

study supports the roles, definitions, and reporting structures identified. As there is no recognized research related to the roles of the CISO within a government contracting organization, this study has delivered on its research purpose and has offered new information that serves to benefit the government contracting community. This research's outcome is the roles, definitions, and reporting structures required for a CISO to successfully establish and maintain a government contractor's information and data security.

CISO Roles

When properly implemented by an organization's executive, cybersecurity, and information technology leadership, the roles identified in this study will help these leaders to understand how the CISO should be positioned with their organization as an executive leader that serves to ensure the resiliency of the business. Additionally, in the case of the government contractor, due to the pressures placed on the organization from new and growing cybersecurity requirements, the CISO serves as a key business enabler by supporting the company's ability to meet government cybersecurity requirements (Nyczepir, 2020). These requirements are used by the government to down select suppliers that cannot meet the criteria. This means that a position like the CISO is required within the government contracting organization to compete for and win new government work successfully. The following tables provide the roles that were ranked by the expert panel and sorted against other elements of study data related to themes and organizational culture theory. Table 50 provides the roles that were organized by the expert panel as being the most critical roles for the CISO within a government contracting organization. The roles are ranked 1 through 9, with one being the most vital role and nine being the least important role.

Table 50

Expert Panel Ranked Roles

Role Ranking	Round 3
1	Risk Management
2	Strategy and Planning
3	Business Partner and Integrator
4	Governance and Compliance
5	Security Knowledge
6	Security Program Management
7	Communications and Marketing
8	Technical Security Operations
9	Security Architecture

Table 51 provides an additional view of the roles ranked by the expert panel. In this table, the roles have been categorized against the major themes identified in this study. Additionally, this table has been sorted based on study themes making it easier to see how the various CISO roles fall into the identified themes. Finally, within each theme, the CISO role has been rank-ordered so that it is apparent which role is ranked as the most essential inside of a theme. This provides additional insight for each role when combined with each theme's narrative responses in chapter five.

Table 51

Ranked CISO Roles Aligned to Study Themes Sorted by Study Theme Ranking

Top Theme Ranking	Themes	Roles	CISO Role Ranking
1	Business Alignment	Strategy and Planning	2
		Business Partner and Integrator	3
2	Program Management	Security Knowledge	5
		Security Program Management	6
		Communications and Marketing	7
3	Risk Management	Risk Management	1
4	Architecture	Technical Security Operations	8
		Security Architecture	9
5	Security Requirements	Governance and Compliance	4

Table 52 provides an additional view of the CISO roles categorized against this study's major themes. This table has been sorted based on the CISO role rank order. This allows the reader to see how the various identified themes aligned with the CISO roles based on the role rank orders.

Table 52

Ranked CISO Roles Aligned to Study Themes Sorted by CISO Role Ranking

Top Theme Ranking	Themes	Roles	CISO Role Ranking
3	Risk Management	Risk Management	1
1	Business Alignment	Strategy and Planning	2
2	Program Management	Business Partner and Integrator	3
5	Security Requirements	Governance and Compliance	4
2	Program Management	Security Knowledge	5
2	Program Management	Security Program Management	6
2	Program Management	Communications and Marketing	7
4	Architecture	Technical Security Operations	8
4	Architecture	Security Architecture	9

Table 53 provides an analysis of CISO roles aligned with organizational culture theory. Foundationally organizational culture theory is the shared beliefs and assumptions held by the individuals who make up the organization (Schein, 1992). From an organizational culture perceptive, culture concepts are applied across an organization at the enterprise level down to the line team member to solve internal and external problems related to mission performance (Schein, 1992).

Table 53

Ranked CISO Roles Aligned with Organizational Culture Theory

Categories	Identified Themes	Ranking Score
Artifacts	Risk Management	1
	Governance and Compliance	4
	Security Architecture	9
Beliefs	Strategy and Planning	2
	Security Program Management	6
	Technical Security Operations	8
Assumptions	Business Partner and Integrator	3
	Security Knowledge	5
	Communications and Marketing	7

Organizational culture theory comprises three levels that allow for further analysis of an organization and how its culture affects its ability to be successful. The first level has to do with organizational artifacts. Artifacts are those things that make up an organization and are associated with something that you hear, feel, and see. The second level of organizational culture theory has to do with the beliefs and values espoused by the organization. The final level of organizational culture theory discusses the basic assumptions taken for granted to be accurate within the organization (Schein, 1992). Based on an understanding of Organizational Culture Theory and the need for leadership to manage and cultivate an effective organizational culture (Marinova et al., 2019), the CISO must work to establish an information security culture that aligns with and supports the organization's culture (Tang et al., 2016). Aligning this study with

organizational culture theory will allow an organization to not merely take the roles and the definitions provided in this study as simply part of a technology program. The cybersecurity program led by the CISO is an integral part of establishing an overall corporate culture centered around security and resiliency for a company.

CISO Role Definitions

The expert panel additionally defined each role that was ranked as part of the study. The researcher synthesized the results from Round 1, where the panel provided a narrative response to define each role that was being ranked. Round 2 then sought to gain consensus on the synthesized definition. If an agreement were not met, the panelist would provide a recommendation for a change. For Round 3, the researcher made changes to the definitions based on panelist's recommendations. All definitions were agreed to by the panel of experts. Below are the definitions for the CISO roles.

Risk Management: Defining, analyzing, and quantifying top cybersecurity risks to revenue, profit, and competitiveness to manage priorities among risks to which funds will be allocated for remediation. This includes developing, operating, and leading while defining, enforcing, and documenting risk - to set and maintain a compliant (and operable) risk posture for the organization. Treatment plans are developed to address risks that are outside of the risk appetite of the organization based on a careful evaluation of threat actors, actor motivation, threats, threat likelihood, vulnerabilities, asset value, asset criticality, and the impact on a system, the organization, or the public. Not all risk can be eliminated from any given environment. The goal of Risk Management is to reduce risk to an acceptable level where the residual risk can be measured and is in alignment with management expectations.

Strategy and Planning: A forward-looking view of the security program's current state, what needs to be accomplished, and the steps necessary to achieve a target state. This is achieved by analyzing the business's needs and the expected evolution of IT within the environment. This leads to the setting of goals and objectives that align the security program with the business's needs, delivering the security program's target state via well-developed security plans easily understood by business leaders. By aligning the security program with corporate goals, a vision and path forward are promoted and integrated with the business's mission.

Business Partner and Integrator: Someone that understands business priorities and challenges so that security is an enabler. They can communicate and partner with members of the business to achieve objectives securely and safely aligned with organizational risk appetite. Business partners and integrators help to address gaps and augment organizational capabilities participating in discussions related to the connection of systems and the flow of business data bringing oversight, monitoring, and secure implementation capabilities to an engagement.

Governance and Compliance: A company's strategy for managing the broad issues of governance, risk management, and corporate compliance with all relevant federal, state, local, and business sector regulatory compliance requirements. This includes ensuring that stakeholder, legal, regulatory, and contractual requirements are evaluated, understood, implemented, and enforced as part of a security program and information system implementation.

Security Knowledge: Ability to understand security, privacy, and compliance concerns in full alignments with the business's needs to protect the confidentiality, integrity, and availability of sensitive information and assets factoring in risks and requirements that an organization has concerning security, privacy, and compliance. Having the competencies required to implement a risk-based security program that incorporates the complex,

interconnected nature of the enterprise environment and maintains a secure, compliant, operationally effective, and efficient security posture

Security Program Management: The leadership (regular, active management) of a program which provides operational roadmaps, security resources, and standards for an organization, in addition to operational capabilities that ensure the selection and implementation of management, operational, and technical security controls commensurate with both the risk and regulatory requirements of the enterprise. Security program management also encompasses the projects, programs, and portfolio management of security-related initiatives that support compliance, risk management, POAM resolution, technology development, policies/procedures, training, and funding which are coordinated to produce a resilient organization.

Communications and Marketing: Evangelizing and disbursing information and ideas to establish buy-in at all organizational levels, about the organization's security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis. The ability to communicate with business stakeholders about the importance and value of security considerations and market the business enabler that a sound security program provides for an organization. Communications and marketing are directed at all levels of the organization to ensure a corporate culture of security is developed and maintained.

Technical Security Operations: The day-to-day operations, maintenance, management, and monitoring of incident response, threat hunting, vulnerability assessment, penetration testing/red teaming, forensics, and disaster recovery services for an organization allowing for risk to be managed to acceptable levels in support of organizational risk management, privacy, and compliance requirements. This capability requires technical depth, leadership, and

business/mission alignment to operate and lead security services that focus on operational delivery.

Security Architecture: Ability to define a framework and plan to implement an architecture and corporate security culture which decreases operational risk, enhances organizational security, and provides security standards for an organization's digital systems and components to address security, privacy, and compliance concerns. Security architecture requires one to think broadly about the interplay of various technology pieces as they develop technical blueprints, which allow for secure solution implementation supporting continuous security monitoring.

CISO Management Reporting Structure

A key area for a company's executive leadership to focus on is the reporting relationship for the CISO. 16 of 17 respondents to this study did agree that the CISO should report to the CEO to ensure transparency and accurate reporting related to digital technology risks. It was noted that the CIO reporting could be acceptable, but there needed to be certain conditions in place for this relationship to work effectively. For the CISO to report to the CIO, the CIO must report directly to the CEO. With this relationship, the CIO must champion cybersecurity and provide transparent reporting to the CEO related to cybersecurity risk. The issue for the company to determine is if the relationship between the CISO and CIO is healthy and that conversations on risk are making it to the broader management team. The CISO serves as the internal assessment/audit function from a cybersecurity perspective. In this role, the CISO is responsible for auditing the technology designed, deployed, and managed by the CIO. This relationship can create a conflict of interest if not managed effectively by the CIO and the firm's executive team.

Figure 50 provides a visual representation of the expert panel responses related to CISO's reporting structure.

Figure 50. CISO Reporting Structure Word Cloud

This research directly contributes to the U.S. government contracting community by understanding the role of the CISO through an exhaustive review of the literature and by conducting a study that brought together industry experts to rank and define the role of the CISO within a U.S. government contracting organization. The respondents also discussed the management structure the CISO should reside under to be effective and drive secure outcomes. The findings documented in this study allow the government supplier to properly align the CISO role within their organization to support their competitiveness and resiliency. The CISO can use this research to better justify the need for cybersecurity within the organization and communicate this with the findings presented in this study. This study's results have not been documented previously in the academic literature and serve to advance the information technology and cybersecurity body of knowledge.

Contribution to Business Technical Problem

The general problem is that government contracting organizations face the threat of not establishing new or maintain existing contractual work as a result of non-compliance with U.S. federal cybersecurity requirements. The specific problem is that executives within government

contracting organizations do not understand how to strategically align the CISO in the government contracting organization in support of an enterprise digital strategy that includes U.S. federal cybersecurity requirements. Discerning what makes up the varied roles of the CISO is critical to the mission of the U.S. federal government contracting organization. While there has been a significant focus on the CISO role from a popular and trade article perspective, there has been little academic research (Karanja & Rosso, 2017). Additionally, after reviewing the limited academic research related to the role of the CISO, no academic research was identified related to the CISO for a government contracting organization. As little academic research exists on the subject of the CISO and no research exists for CISO within government contracting organizations, this avenue of research provided an excellent opportunity to offer a meaningful study and analysis to further the overall body of knowledge related to information technology management and cybersecurity.

This research directly contributes to the federal government's goals related to contractor security and supply chain management in addition to supplying the government contractor with the information needed to align the CISO role more effectively within their organizations. The information provided by this research in the form of a literature review, roles, role definitions, and CISO reporting structure serves to provide the government contracting organization with the information needed to ensure that cybersecurity is integrated into the organization. Once integrated, cybersecurity activities can be led by an appropriate leader that can combine both the technical and business aspects of cybersecurity to manage risk and drive organizational resiliency. By aligning the study with organizational culture theory, this research provides a blueprint for organizational change that will drive the organizational culture to secure outcomes. Organizational culture is significant in developing and sustaining an effective information

security program (Tang et al., 2016). Additionally, information security leadership in the form of the chief information security officer directly affects and influences organizational and information security culture to develop and lead information security program development.

Recommendations for Further Research

Cybersecurity requirements are rapidly evolving in the government contracting industry. This evolution presents some exciting opportunities for further research to be conducted. The varied cybersecurity requirements that have been developed across the U.S. federal government offer an opportunity to conduct research. This area of research would focus on the financial impact of implementing cybersecurity requirements for a federal contractor. As effective cybersecurity measures cost the organization time and money, a study that reviews this impact would be beneficial. Another potential area of research related to government cybersecurity requirements is to develop a crosswalk of requirements that would help the community to understand the commonalities across government requirements. The study would create a combined framework that would allow the government contractor community to understand the high watermark across government cybersecurity requirements assisting the contractor with a more straightforward implementation of multiple cybersecurity requirement frameworks. A final area of research to be considered is to understand the CIO's role as it relates to the implementation of the government's cybersecurity requirements. This would be interesting research as it could be used to compare and contrast the CISO and the CIO's role, focusing on the specific undertaking of bringing an organization into compliance with federal government cybersecurity requirements.

Conclusion

This qualitative Delphi study has provided an understanding of the roles needed for a CISO to be successful in establishing and maintaining a government contracting organization's information and data security. This was accomplished through the development of an exhaustive literature review on the role of the CISO. This literature review informed the researcher related to the roles that drive success for cybersecurity leaders. These roles were then taken and provided to an expert panel of government contracting cybersecurity leaders that ranked them related to importance. Additionally, this panel of experts defined the roles so that a better understanding could exist related to the panel's understanding of the roles they were ranking and so that the readers of this study could more readily implement the roles within their organization. Finally, an analysis of the CISOs managerial reporting relationships was reviewed, providing recommendations for the optimal reporting relationship. This study provides the government supplier with the information needed to align cybersecurity and the CISO properly within their organizations.

References

American Institute of Certified Public Accountants (AICPA). (2018). *Traits of today's CFO: A handbook for excelling in an evolving role.* John Wiley & Sons, Incorporated.

Alexander, A., & Cummings, J. (2016). The rise of the chief information security officer. *People & Strategy 39*(1), Winter2016, pp 10-13.

Andriole, S. J. (2017). Five myths about digital transformation. *MIT Sloan Management Review, 58*(3), 20.

Armstrong, M. (2017). *Armstrong's handbook of human resource management practice* (14th ed). New York: Kogan Page Limited.

Akins, R. B., Tolson, H., & Cole, B. R. (2005). Stability of response characteristics of a Delphi panel: Application of bootstrap data expansion. *BMC Medical Research Methodology, 5*(1), 37-37. doi:10.1186/1471-2288-5-37

Bak, O. (2018). Supply chain risk management research agenda: From a literature review to a call for future research directions. *Business Process Management Journal, 24*(2), 567-588. doi:10.1108/BPMJ-02-2017-0021

Banks, J.A., & McGee-Banks, C.A. (1989). *Multicultural education: Issues and perspectives.* Simon & Schuster.

Bernard, T. S., Hsu, T., Perlroth, N., & Lieber, R. (2017). *Equifax says cyberattack may have affected 143 million in the US.* Retrieved from https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26*(13), 1802-1811. doi:10.1177/1049732316654870

Brekke, I., & Cassidy, S. (2019). *Readying security plans for evaluation.* Retrieved from https://www.nationaldefensemagazine.org/articles/2019/1/30/readying-security-plans-for-evaluation.

Boggs, W. B. (2004). TQM and organizational culture: A case study. *Quality Management Journal, 11*(2), 42-52. doi:10.1080/10686967.2004.11919110

Browning, G. (2018). *Work that works: Emergineering a positive organizational culture.* NJ: John Wiley & Sons, Inc.

Bryman, A. (2012). *Social research methods,* (4th ed). NY: Oxford University Press.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36-45. doi:10.1016/j.jisa.2018.08.002

Caldwell, T. (2017). The UK's £1.9bn cyber-security spend – Getting the priorities right. *Computer Fraud & Security, 2017*(3), 12-20. doi:10.1016/S1361-3723(17)30024-6

Cameron, K., & Quinn, R. (2006). *Diagnosing and changing organizational culture: Based on the competing values framework.* NJ: Jossey-Bass.

Candela, A. G. (2019). Exploring the function of member checking. *Qualitative Report, 24*(3), 619-628.

Carper, T. (2014). S.2521 - *113th congress (2014): Federal information security modernization act of 2014.* Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521.

Carter, L., Weerakkody, V., Phillips, B., & Dwivedi, Y. K. (2016). Citizen adoption of e-government services: Exploring citizen perceptions of online services in the United States and United Kingdom. *Information Systems Management, 33*(2), 124-140. doi:10.1080/10580530.2016.1155948

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability, 8*(7), 638. doi:10.3390/su8070638

Chokshi, N. (2019). *Attacked with ransomware, Baltimore isn't giving in.* Retrieved From https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html.

Coburn, A., Leverett, E., & Woo, G. (2019). *Solving cyber risk: protecting your company and society.* NJ: John Wiley & Sons, Inc.

CompTIA. (2018). *IT industry outlook 2018.* Retrieved from https://www.comptia.org/resources/it-industry-trends-analysis.

Cooper, D. R., & Schindler, P. S. (2014). *Business research methods.* NY: McGraw-Hill/Irwin.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches.* (5th ed.). CA: Sage Publications.

Crumpler, W., & Lewis, J. (2019). *The cybersecurity workforce gap.* Retrieved from https://www.csis.org/analysis/cybersecurity-workforce-gap.

Cyber Seek. (2020). *Cybersecurity supply and demand heat map.* Retrieved from https://www.cyberseek.org/heatmap.html.

Cyberspace Solarium Commission. (2020). Cyberspace solarium commission report. Retrieved from https://www.solarium.gov/report

Dahlberg, L., & McCaig, C. (2010). *Practical research and evaluation: A start-to-finish guide for practitioners.* CA: Sage.

Death, D. (2017). *Information security handbook: Develop a threat model and incident response strategy to build a strong information security framework.* UK: Packt Publishing.

Death, D. (2019). *A new report on the compliance impact of new federal rules on cybersecurity contractors.* Retrieved from https://securitycurrent.com/aligning-corporate-executives-with-us-federal-government-regulations-associated-with-contractor-and-supply-chain-security-requirements/.

DOD. (2019). *Cybersecurity maturity model certification.* Retrieved from https://www.acq.osd.mil/cmmc/draft.html.

Doherty, N. F., Ashurst, C., & Peppard, J. (2012). Factors affecting the successful realisation of benefits from systems development projects: Findings from three case studies. *Journal of Information Technology, 27(*1), 1-16. doi:10.1057/jit.2011.8

Dombora, S. (2016). Characteristics of information security implementation methods. *Management, Enterprise and Benchmarking in the 21st Century, 57.*

Doubleday, J. (2019). *Defense dept. to require new cybersecurity certification from contractors.* Inside Cybersecurity. Retrieved from https://insidecybersecurity.com/daily-news/defense-dept-require-new-cybersecurity-certification-contractors.

Fazzini, K. (2019). *Equifax just became the first company to have its outlook downgraded for a cyber-attack.* Retrieved from https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html.

FBI. (2018). *2017 Internet crime report.* Retrieved from https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718.

Fletcher, B., & Jones, F. (1992). Measuring organizational culture: The cultural audit. *Managerial Auditing Journal, 7*(6), 30–32. doi:10.1108/eb017606

Freedberg, S. (2019). *Protect your data or lose DOD business.* Retrieved from https://breakingdefense.com/2019/12/protect-your-data-or-lose-dod-business-maj-gen-murphy-exclusive/.

Ghauri, P., & Gronhaug, K. (2010). *Research methods in business studies: A practical guide.* (4th ed.). Harlow, England: FT-Pearson.

Gikas, C. (2010). A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS standards. *Information Security Journal: A Global Perspective, 19*(3), 132-141. doi:10.1080/19393551003657019

Goel, S., Williams, K., Dincelli, E., & University at Albany, S. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44. doi:10.17705/1jais.00447

Granneman, J. (2018). The business guide to improving information security. *The Journal of Equipment Lease Financing (Online), 36*(3), 1-9.

Gregor, S., & Lee-Archer, B. (2016). The digital nudge in social security administration. *International Social Security Review, 69*(3-4), 63-83. doi:10.1111/issr.12111

Griffy-Brown, C., Lazarikos, D., & Chun, M. (2019). Emerging technologies and cyber risk: How do we secure the internet of things (IoT) environment? *Journal of Applied Business and Economics, 21*(2), 70-79. doi:10.33423/jabe.v21i1.1455

Gunzel, J. A. (2017). Tackling the cyber threat: The impact of the dod's "network penetration reporting and contracting for cloud services" rule on dod contractor cybersecurity. *Public Contract Law Journal, 46*(3), 687.

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008-1015. doi:10.1046/j.1365-2648.2000.t01-1-01567.x

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management, 43*, 165-172. doi:10.1016/j.ijinfomgt.2018.07.013

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*(6), 585-591. doi:10.1016/j.bushor.2016.07.004

Howles, T., Romanowski, C., Mishra, S., & Raj, R. K. (2011). A holistic, modular approach to infuse cybersecurity into undergraduate computing degree programs. *In Annual Symposium On Information Assurance (ASIA)*, Albany, NY (pp. 7-8).

Hsu, C., & Sandford, B. A. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research & Evaluation, 12*(10), 1-8.

Hulitt, E., & Vaughn, R. B. (2010). Information system security compliance to FISMA standard: A quantitative measure. *Telecommunication Systems, 45*(2-3), 139-152. doi:10.1007/s11235-009-9248-8

International Organization for Standardization (ISO). (2019). ISO/IEC 27001 Information security management. Retrieved from https://www.iso.org/isoiec-27001-information-security.html.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information and Computer Security, 25*(3), 300-329. doi:10.1108/ICS-02-2016-0013

Karanja, E., & Rosso, M. A. (2017). the chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, *26*(2), 23-47.

Karimi-Alaghehband, F., & Rivard, S. (2014). Air Canada: Flying High with Information Technology. *International Journal of Case Studies in Management, 12*(2). Retrieved From https://services.hbsp.harvard.edu/api/courses/664856/items/HEC045-PDF-ENG/sclinks/76bc4a75eaa17e64e32c7c7c3e048e20.

Keeney, S., Hasson, F., & McKenna, H. (2006). Consulting the oracle: Ten lessons from using the delphi technique in nursing research. *Journal of Advanced Nursing, 53*(2), 205-212. doi:10.1111/j.1365-2648.2006.03716.x

Kennedy, S. E. (2016). The pathway to security – Mitigating user negligence. *Information and Computer Security, 24(*3), 255-264. doi:10.1108/ICS-10-2014-0065

Kulkarni, M. (2018). IT governance in global banks: Emerging models. *Vinimaya, 39*(1), 11-21.

Kure, H., Islam, S., & Razzaque, M. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences, 8*(6), 898. doi:10.3390/app8060898

Lange, R., & Burger, E. (2017) Long-term market implications of data breaches, not, *Journal of Information Privacy and Security, 13*(4), 186-206, DOI: 10.1080/15536548.2017.1394070

Lanz, J. (2017). The chief information security officer: The new CFO of information security. The CPA Journal, 87(6), 52-57.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. doi:10.1016/j.ijinfomgt.2018.10.017

Lops, P., De Gemmis, M., Semeraro, G., Narducci, F., & Musto, C. (2011). Leveraging the LinkedIn social network data for extracting content-based user profiles. *In Proceedings of the fifth ACM conference on Recommender systems (pp. 293-296)*. ACM. doi: 10.1145/2043932.2043986

Lyngaas, S. (2019). *'It's going to be painful': Pentagon official urges contractors to improve cybersecurity.* Retrieved from https://www.cyberscoop.com/katie-arrington-pentagon-contracting/.

MacIntosh, E., & Doherty, A. (2009). The influence of organizational culture on job satisfaction and intention to leave. *Sport Management Review, 13*(2), 106–117. doi:10.1016/j.smr.2009.04.006

Marinova, S. V., Cao, X., & Park, H. (2019). Constructive organizational values climate and organizational citizenship behaviors: A configurational view. *Journal of Management, 45*(5), 2045-2071. doi:10.1177/0149206318755301

Maynard, S. B., Onibere, M., & Ahmad, A. (2018). Defining the strategic role of the chief information security officer. *Pacific Asia Journal of the Association for Information Systems, 10*(3), pp. 61-86.

Mithas, S., Rust, R. T., & University of Maryland. (2016). How information technology strategy and investments influence firm performance: conjecture and empirical evidence. *MIS Quarterly, 40*(1), 223-245. doi:10.25300/MISQ/2016/40.1.10

Morgeson, F. V., & Petrescu, C. (2011). Do they all perform alike? An examination of perceived performance, citizen satisfaction and trust with US federal agencies. *International Review of Administrative Sciences*, *77*(3), 451-479. doi:10.1177/0020852311407278

Murphy, S. P. (2018). A holistic approach to cybersecurity starts at the top. *Frontiers of Health Services Management, 35*(1), 30-36. doi:10.1097/HAP.0000000000000041

Nadella, S. (2019). Annual Report 2019. Retrieved from https://www.microsoft.com/investor/reports/ar19/index.html.

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12-22. doi:10.1016/j.jisa.2018.11.003

National Institutes of Standards and Technology. (NIST) (2001). *Security requirements for cryptographic modules*. Retrieved From https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

National Institute of Standards and Technology (NIST). (2004). *Standards for security categorization of federal information and information systems.* Retrieved from https://csrc.nist.gov/publications/detail/fips/199/final.

Nyczepir, D. (2020). GSA adding supply chain requirements to major contracts. Retrieved from https://www.fedscoop.com/gsa-supply-chain-requirements-gwacs/.

Office of Management and Budget (OMB). (2017). *Report to the president on federal IT modernization,* Retrieved from https://itmodernization.cio.gov/.

Ogutu, J., Bennett, M. R., & Olawoyin, R. (2018). Closing the gap: between traditional & enterprise risk management systems. *Professional Safety, 63*(4), 42-47.

O'Neill, P. H. (2017). *Booz Allen Hamilton leaves 60,000 unsecured dod files on AWS server.* Retrieved from https://www.cyberscoop.com/booz-allen-hamilion-amazon-s3-chris-vickery/.

Payscale.com. (2019). *Average chief information security officer salary in washington, district of columbia.* Retrieved from https://www.payscale.com/research/US/Job=Chief_Information_Security_Officer/Salary/ab64d8e8/Washington-DC.

Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., & Stavrou, E. (2018). *Global perspectives on cybersecurity education.* doi:10.1145/3197091.3205840

Pettigrew, A. M. (1979). On studying organizational cultures. *Administrative Science Quarterly, 24*(4), 570-581. doi:10.2307/2392363

Plachkinova, M., & Maurer, C. (2018). Security breach at Target. *Journal of Information Systems Education, 29*(1), 11-19.

Ponemon Institute. (2018). 2018 study on global megatrends in cybersecurity Retrieved from https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf.

Pullin, D. W. (2018). Cybersecurity: Positive changes through processes and team culture. *Frontiers of Health Services Management, 35*(1), 3-12. doi:10.1097/HAP.0000000000000038

RAND Corporation. (2016). *Delphi Method.* Retrieved from: https://www.rand.org/topics/delphi-method.html.

Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity: Building a successful defense program. *Frontiers of Health Services Management, 35*(1), 13-22. doi:10.1097/HAP.0000000000000037

Ross, R., Dempsey, K., Viscuso, P., Riddle, M., & Guissanie, G. (2018). *Protecting controlled unclassified information in nonfederal systems and organizations.* Retrieved from https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

Rothrock, R. A., Kaplan, J., & Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12-15.

Sabherwal, R., Sabherwal, S., Havaknor, T., Steelman, Z., University of Arkansas, University of Texas-Arlington, & Temple University. (2019). How does strategic alignment affect firm performance? The roles of information technology investment and environmental uncertainty. *MIS Quarterly, 43*(2), 453-474. doi:10.25300/MISQ/2019/13626

Santos-Olmo, A., Sánchez, L., Caballero, I., Camacho, S., & Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet, 8*(4), 30. doi:10.3390/fi8030030

Schein, E. H. (1992). *Organizational culture and leadership* (2nd ed.). CA: Jossey-Bass.

Schein, E. H. (2017). *Organizational culture and leadership* (Fifth ed.). NJ: Wiley.

Schein, E. H., & Schein, P. A. (2019). *The corporate culture survival guide* (3rd ed.). NJ: John Wiley & Sons, Inc.

Scott, T., & Daniels, M. (2016). *Announcing the first federal chief information security officer.* Retrieved from https://obamawhitehouse.archives.gov/blog/2016/09/08/announcing-first-federal-chief-information-security-officer.

Smith, B. H., Torrance, N., Ferguson, J. A., Bennett, M. I., Serpell, M. G., & Dunn, K. M. (2012). Towards a definition of refractory neuropathic pain for epidemiological research. An international delphi survey of experts. *BMC Neurology, 12*(1), 29-29. doi:10.1186/1471-2377-12-29

Sosin, A. (2018). How to increase the information assurance in the information age. *Journal of Defense Resources Management, 9*(1), 45-57.

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security, 25*(5), 494-534. doi:10.1108/ICS-07-2016-0054

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society, 71*, 15-29. doi:10.1016/j.aos.2018.04.005

Sweeney, B. E. (2018). The nexus between cyber and ethics. *National Defense, 103*(780), 38-38.

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management, 17*(2), 179-186. doi:10.1007/s10799-015-0252-2

Trope, R. L. (2018). When incident response goes awry: Cybersecurity developments. *Business Lawyer, 74*(1), 229.

Verizon. (2019). *2019 Data breach investigations report.* Retrieved from https://enterprise.verizon.com/resources/reports/dbir/.

Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. *Association for Computing Machinery. Communications of the ACM, 62*(4), 120-120. doi:10.1145/3241037

Webb, J., Ahmad, A., Maynard, S., & Shanks, G. (2016). Foundations for an intelligence-driven information security risk management system. *Journal of Information Technology Theory and Application, 17*(3), 25-51. doi:10.3127/ajis.v8i3.1096

Whissemore, T. (2018). Guarding against cybercrime. *Community College Journal, 89*(2), 31-31.

Whitehouse.gov. (2018). *President Donald J. Trump signed HR.R. 3359 into law.* Retrieved from https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-signed-h-r-3359-law/.

Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems, 48*(3), 15-19. doi:10.1080/08874417.2008.11646017.

Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications, 7*(1), 1-12. doi:10.1186/s13174-016-0046-8

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). NY: Guilford Press.

Zimba, A., & Chishimba, M. (2019). Understanding the evolution of ransomware: paradigm shifts in attack structures. *International Journal of Computer Network and Information Security, 11*(1), 26-39. doi:10.5815/ijcnis.2019.01.03

APPENDIX A. DEMOGRAPHIC QUESTIONAIRE

Question 1: How many years have you held the role of CISO (or equivalent position) for a government contracting organization?

Question 2: Where did your CISO (or equivalent position) report to within the organization?

Question 3: How many years of experience do you have in the information technology field?

Question 4: What is your current position?

Question 5: What certification do you have?

APPENDIX B. ROUND 1 QUESTIONAIRE

Question 1: Explain your role as a cybersecurity leader.

Question 2: Rank the below roles in order of importance for the CISO.

- Business Partner and Integrator
- Technical Security Operations
- Security Architecture
- Security Program Management
- Governance and Compliance
- Risk Management
- Communications and Marketing
- Strategy and Planning
- Security Knowledge

Question 3: Define Business Partner and Integrator in your own words.

Question 4: Define Technical Security Operations in your own words.

Question 5: Define Security Architecture in your own words.

Question 6: Define Security Program Management in your own words.

Question 7: Define Governance and Compliance in your own words.

Question 8: Define Risk Management in your own words.

Question 9: Define Communications and Marketing in your own words.

Question 10: Define Strategy and Planning in your own words.

Question 11: Define Security Knowledge in your own words.

Question 12: For the top five roles identified in question one, describe why these roles made it into your list of top roles.

Question 13: Where should the CISO report within the organization to achieve the greatest effectiveness?

- CEO
- CTO
- CIO
- Other

Question 14: For your selection in question four please describe how this reporting structure will serve to contribute to the success of the CISO and security of the business?

Question 15: Is there any additional information you would like to provide related to the role of the CISO that will empower the CISO to succeed within an organization?

APPENDIX C. ROUND 2 QUESTIONAIRE

Question 1: Based on the responses of the study's participants the roles needed by the CISO are ranked below. 1 = Most Important 9 = Least Important.

1. Risk Management
2. Strategy and Planning
3. Business Partner and Integrator
4. Governance and Compliance
5. Security Knowledge
6. Security Program Management
7. Technical Security Operations
8. Communications and Marketing
9. Security Architecture

Do you agree with this ranking?

1. Yes
2. No

If you do not agree with the above ranking what would you change?

Question 2: Do you agree with the below definition of Business Partner and Integrator?

Definition: Someone that understands business priorities and challenges so that security is an enabler. They can communicate and partner with members of the business to achieve objectives securely and safely aligned with organizational risk appetite. Business partners and integrators help to address gaps and augment organizational capabilities participating in discussions related to the connection of systems and the flow of business data bringing oversight, monitoring, and secure implementation capabilities to an engagement.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 3: Do you agree with the below definition of Technical Security Operations?

Definition: Technical security operations are the day-to-day maintenance, management, and monitoring of incident response, threat hunting, vulnerability assessment, penetration testing/red teaming, forensics, and disaster recovery services for an organization allowing for risk to be managed to acceptable levels in support of organizational risk management and compliance requirements. This capability requires technical depth, leadership, and business/mission alignment with the ability to operate and lead security services that focus on operational delivery.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 4: Do you agree with the below definition of Security Architecture?

Definition: Ability to define a framework and plan to implement an architecture and corporate security culture which decreases operational risk, enhances organizational security, and provides security standards for an organization’s digital systems and components to address security,

privacy, and compliance concerns. Security architecture requires one to think broadly about the interplay of various technology pieces as they develop technical blueprints, which allow for secure solution implementation supporting continuous security monitoring.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 5: Do you agree with the below definition of Security Program Management? Definition: The leadership (regular, active management) of a program which provides operational roadmaps, security resources, and standards for an organization, in addition to operational capabilities that ensure the selection and implementation of management, operational, and technical security controls commensurate with both the risk and regulatory requirements of the enterprise. Security program management also encompasses the projects, programs, and portfolio management of security-related initiatives that support compliance, risk management, POAM resolution, technology development, policies/procedures, training, and funding which are coordinated to produce a resilient organization.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 6: Do you agree with the below definition of Governance and Compliance?

Definition: A company's strategy for managing the broad issues of governance, risk management, and corporate compliance with all relevant federal, state, and local regulatory compliance requirements. This includes ensuring that stakeholder, legal, regulatory, and contractual requirements are evaluated, understood, and implemented as part of a security program and systems implementation.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 7: Do you agree with the below definition of Risk Management?

Definition: Defining and analyzing top risks to revenue, profit, and competitiveness for an organization working to manage priorities among risks to which funds will be allocated for remediation. This includes the ability to develop, operate and lead while defining, enforcing, and documenting risk - in an effort to set and maintain a compliant (and operable) risk posture for the organization. Treatment plans are developed to address risks that are outside of the risk appetite of the organization based on a careful evaluation of threat actors, actor motivation, threats, threat likelihood, vulnerabilities, asset value, asset criticality, and the impact on a system, the organization, or the public. Not all risk can be eliminated from any given environment. The goal

of Risk Management is to reduce risk to an acceptable level where the residual risk can be measured and is in alignment with management expectations.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 8: Do you agree with the below definition of Communications and Marketing?

Definition: Evangelizing and disbursing information and ideas to establish buy-in at all organizational levels, about the organization's security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis. The ability to communicate with business stakeholders about the importance and value of security considerations and market the business enabler that a sound security program provides for an organization. Communications and marketing are directed at all levels of the organization to ensure a corporate culture of security is developed and maintained.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 9: Do you agree with the below definition of Strategy and Planning?

Definition: A forward-looking view of the current state of the security program, what needs to be accomplished, and the steps to achieve a target state. This is achieved by analyzing the needs of the business and setting appropriate goals and objectives that serve to deliver the security program's target state via well-developed security plans that are easily understood by business leaders. By aligning corporate goals with those of the security program, a vision and path forward are promoted that is aligned and integrated with the mission of the business.

- Strongly Agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 10: Do you agree with the below definition of Security Knowledge?

Definition: Ability to understand technical security issues and concerns in conjunction with business operations considering risks and requirements that an organization has concerning security, privacy, and compliance. Having the expertise and technical background to implement a security posture that is triaged from a risk management perspective and considers the complexity and interconnectivity of the enterprise environment to maintain the business in a secure, compliant, and operational manner.

- Strongly Agree
- Agree
- Neither agree nor disagree

- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 11: Based on the responses of the study's participants where the CISO should report in the organization is ranked below. 1 = Most Important 2 = Least Important.

1. CEO
2. CIO

Do you agree with this ranking?

1. Yes
2. No

If you do not agree with the above ranking what would you change?

Question 12: Is there any additional information you would like to provide related to the role of the CISO that will empower the CISO to succeed within an organization?

APPENDIX D. ROUND 3 QUESTIONAIRE

Question 1: Based on the responses of the study's participants, the roles needed by the CISO are ranked below. 1 = Most Important 9 = Least Important.

1. Risk Management
2. Strategy and Planning
3. Business Partner and Integrator
4. Governance and Compliance
5. Security Knowledge
6. Security Program Management
7. Communications and Marketing
8. Technical Security Operations
9. Security Architecture

Do you agree with this ranking?

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above ranking how would you change the ranking order?

Question 2: Do you agree with the below definition of Technical Security Operations?

Definition: The day-to-day operations, maintenance, management, and monitoring of incident response, threat hunting, vulnerability assessment, penetration testing/red teaming, forensics, and disaster recovery services for an organization allowing for risk to be managed to acceptable levels in support of organizational risk management, privacy, and compliance requirements. This

capability requires technical depth, leadership, and business/mission alignment to operate and lead security services that focus on operational delivery.

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 3: Do you agree with the below definition of Governance and Compliance?

Definition: A company's strategy for managing the broad issues of governance, risk management, and corporate compliance with all relevant federal, state, local, and business sector regulatory compliance requirements. This includes ensuring that stakeholder, legal, regulatory, and contractual requirements are evaluated, understood, implemented, and enforced as part of a security program and information system implementation.

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 4: Do you agree with the below definition of Risk Management?

Definition: Defining, analyzing, and quantifying top cybersecurity risks to revenue, profit, and competitiveness to manage priorities among risks to which funds will be allocated for remediation. This includes developing, operating, and leading while defining, enforcing, and documenting risk - to set and maintain a compliant (and operable) risk posture for the

organization. Treatment plans are developed to address risks that are outside of the risk appetite of the organization based on a careful evaluation of threat actors, actor motivation, threats, threat likelihood, vulnerabilities, asset value, asset criticality, and the impact on a system, the organization, or the public. Not all risk can be eliminated from any given environment. The goal of Risk Management is to reduce risk to an acceptable level where the residual risk can be measured and is in alignment with management expectations.

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 5: Do you agree with the below definition of Communications and Marketing?

Definition: Evangelizing and disbursing information and ideas to establish buy-in at all organizational levels, about the organization's security program, its policies, and its strategy, both in a singular context and in the context of business requests for review, oversight, or budgetary analysis. The ability to communicate with business stakeholders about the importance and value of security considerations and market the business enabler that a sound security program provides for an organization. Communications and marketing are directed at all levels of the organization to ensure a corporate culture of security is developed and maintained.

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 6: Do you agree with the below definition of Strategy and Planning?

Definition: A forward-looking view of the security program's current state, what needs to be accomplished, and the steps necessary to achieve a target state. This is achieved by analyzing the business's needs and the expected evolution of IT within the environment. This leads to the setting of goals and objectives that align the security program with the business's needs, delivering the security program's target state via well-developed security plans easily understood by business leaders. By aligning the security program with corporate goals, a vision and path forward are promoted and integrated with the business's mission.

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 7: Do you agree with the below definition of Security Knowledge?

Definition: Ability to understand security, privacy, and compliance concerns in full alignments with the business's needs to protect the confidentiality, integrity, and availability of sensitive information and assets factoring in risks and requirements that an organization has concerning security, privacy, and compliance. Having the competencies required to implement a risk-based security program that incorporates the complex, interconnected nature of the enterprise environment and maintains a secure, compliant, operationally effective, and efficient security posture.

- Strongly Agree

- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above definition what would you change?

Question 8: The study's participants identified the below roles as being the optimal managerial reporting relationship for the CISO.

3. CEO
4. CIO

Do you agree with this ranking?

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree

If you do not agree with the above ranking what would you change?

Question 9: Is there any additional information you would like to provide related to the role of the CISO that will empower the CISO to succeed within an organization?