IDENTIFYING LIMITATIONS FROM ORGANIZATIONS IMPLEMENTING NIST SP 800-171

by

Christopher Opp

AHMAD MOSTAFA, PhD, Committee Chair

STEVEN MUNKEBY, DM, Committee Member

DANIEL SMITH, PhD, Committee Member

Cheryl Boncuore, PhD, Interim Dean

School of Business, Technology, and Health Care Administration

A Capstone Project Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Information Technology

Capella University

December 2023

Executive Summary

1.0 Problem. According to recent surveys conducted by the company Sera-Brynn, of the organizations implementing the NIST SP 800-171, nearly 80% are unable (Sera-Brynn, 2019). All 800-171 requirements must be satisfied to protect our nation's data from unauthorized access (RSI Security, 2021).

2.0 Purpose. To gather implementation limitations from organizations implementing NIST SP 800-171 requirements.

3.0 Method. The research outlined in this capstone was completed using qualitative inquiry. Experts from the field were interviewed to determine their experience with limitations from organizations implementing NIST SP 800-171.

4.0 Population. The study interviewed IT professionals who have or have attempted to apply NIST SP 800-171 requirements in their organization. Gathering samples was completed through convenience sampling due to the ability to include the 12 participants based on their specific characteristics. The sample group comprised subject matter experts (Ginn & Munn, 2019). Recruiting was completed using a system called User Interviews, Inc., where requirements were input, and User Interviews, Inc. provided participants. Once the list of participants was provided, I confirmed that the participants met the inclusion and exclusion requirements to be part of the study and eliminated any potential participants who did not. Once the interview session began, I also asked the participants to self-attest that they met these requirements. The inclusion criteria were IT professionals with at least 1 year of experience in the IT field who have attempted or have implemented NIST SP 800-171, and the exclusion criteria are non-IT professionals or professionals who do not have 1 year of experience in the IT field or have not attempted to or implemented NIST SP 800-171.

5.0 Results. This study suggested that organizations encounter limitations when implementing the NIST SP 800-171 guidelines, captured through data analysis based on the guidance of Braun and Clarke (2006) by creating eight themes: user education, ease of enforcement, aspects of business culture, clarity of requirements, conflicting requirements, framework shortfalls, information system shortfalls, and lack of resources. These themes encompassed a variety of specific limitations that organizations are dealing with, including factors internal to the organization and some external. Aspects of business culture, for example, includes ideas such as employee attitudes, management buy-in, and limited skillsets of employees. Framework shortfalls represent future improvements, insufficiency, and scalability difficulties.

6.0 Implications/Practical Uses. Practitioners in the field can use this study's results to aid in addressing the limitations they are experiencing in their organizations. Understanding the more significant overall themes derived from these limitations and helping to determine where to start when addressing them can help stakeholders in their organizations. Finding creative ways to address these limitations can help organizations implement these tools, increasing overall security and enabling them to continue maintaining their business practices. Scholars can similarly use this study to build upon previous studies, find creative ways to address limitations, and find a starting point for their research projects.

Dedication

For my dear and wonderful wife, who has always been there through thick and thin and has been a partner in every one of my journeys, including this one.

Acknowledgments

Writing this capstone has been a journey, and I would like to thank my professors, my committee members, and my interview participants, who have all been crucial to the completion of this study.

Table of Contents

List of Tables

List of Figures

SECTION 1. BUSINESS TECHNICAL PROBLEM AND PROJECT SCOPE

1.1 Introduction

Organizations have created essential security tools that are available and often mandated for business data security (Mutune, 2022). These tools are often required based on a company's handling of data, and one group of companies like this are organizations responsible for working with CUI data (Spencer, 2019). The ability of these companies to receive and generate CUI data, which can negatively impact the security of the United States, means that there is a requirement to follow specific laws and publications (Peters, 2022). A prime example of this is the National Institute of Standards and Technology (NIST) requires companies that work with government contracts to follow the cybersecurity policies and requirements that were created to address a requirement leveraged by the Federal Acquisition Regulation (FAR) and further delegated to organizations through the use of the Defense Federal Acquisition Regulation Supplements (DFARS) (Spencer, 2019). Along with the FAR and DFARS, there are further requirements that are required by the NIST through the use of the NIST's Special Publication 800-171 (Ross et al., 2021). Having products such as the NIST SP 800-171 available for organizations to implement helps organizations implement features in their information systems to protect data (NIST, 2018). However, while these tools have been developed, the information shows that organizations cannot fully implement these tools (Sera-Brynn, 2019). There is a gap in understanding why the NIST SP 800-171 tool exists and why the tool is not being fully implemented in organizations that are required to implement these technologies.

1.2 Capstone Topic

Although government contracting organizations are required to implement NIST’s Publication 800-171 and other cybersecurity policies, cybersecurity threats are continually changing and increasing (Jakkal, 2022). Organizations must implement NIST's Publication 800-171 and other cybersecurity policies and requirements and recognize that there needs to be a change in the application of cybersecurity (Clarke & Knake, 2020; Sundararajan, 2022). With the U.S. Government realizing that organizations have been unable to fully comply with the NIST SP 800-171 requirements, they leveraged the Under Secretary of Defense Acquisition and Sustainment Division (OUSDAS) to create a new model titled the cybersecurity maturity model certification, or CMMC (Henry, 2015; Imsand et al., 2019). The CMMC model was created by using the NIST SP 800-171, among other cybersecurity documents, to create an up-to-date list of cybersecurity requirements for the United States. Implementing a new model based on the old 800-53 model while additionally requiring a third-party audit system represents the Government's attempt to address limitations organizations face when implementing their tools (OUSDAS, 2020). Compliance with the NIST SP 800-171 has not been implemented by all government contractors (Sera-Brynn, 2019). According to the OUSDAS, 'The goal is for the CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels, and the intent is for certified, independent third-party organizations to conduct audits and inform risk' (OUSDAS, 2020, para. 5). With the requirement in place for organizations to implement the 800-171 and reviewing reports from outside organizations it appears that there is some piece of knowledge that is missing that is creating limitations for these companies from implementing these tools (NIST, 2019). Considering this lack of knowledge and with the Government's attempts to overhaul the process through revisions such as creating the new CMMC model, it further becomes apparent that limitations are holding up the entire 800-171 implementation.

Researchers from the U.S. Government and non-government organizations have conducted initial studies investigating contractor organizations' abilities to implement and comply with the CSF (Troia, 2018). Although studies have been completed on a variety of tools, the NIST SP 800-171 specifically has not been addressed. With this lack of research, a gap in knowledge existed relating to the limitations in implementing the NIST SP 800-171 requirements.

1.2.1 Problem of Practice

This project addressed the fact that organizations have found it challenging to realize a fully compliant information system in which they are able to handle CUI on behalf of the U.S. government (Sera-Brynn, 2019). When organizations encounter limitations, such as being unable to fully implement the NIST 800-171 requirements, overall cybersecurity strength is affected since these frameworks are created to help reduce vulnerabilities (Chancey, 2022). When limitations are encountered, organizations are forced to choose between not implementing or partially implementing the expected cybersecurity requirements (Alahmari & Duncan, 2020). Evaluating these limitations as risks and then deciding which risks to accept, transfer, or mitigate is a large part of what cybersecurity professionals do today (Pandey et al., 2020).

Knowing these limitations means an IT professional is able to identify the risk created by the limitation; the limitations are not consistently recognized by different organizations or captured in a way that can be used to help organizations solve these implementation issues associated with the limitations (Bergström et al., 2019). The specific problem was that organizations did not know what limitations existed when implementing the NIST SP 800-171, which made it difficult or impossible for IT professionals to implement the requirements

(Purplesec, 2022). Not knowing what limitations exist causes the IT professional to be unprepared and can lead to a failure in the implementation of these requirements.

1.3 Purpose of the Project

Using the qualitative inquiry process, the question, “What are the implementation limitations IT professionals must resolve for NIST SP 800-171 compliance?” was answered. Interviewing IT professionals in the field to gather perspectives to learn the compliance limitations causing organizations to have difficulty implementing these requirements.

1.3.1 Project Need

IT leaders benefit from more information and collaboration regarding limitations to overcome the difficulties organizations are experiencing when implementing NIST SP 800-171 (Xie, 2020). A qualitative inquiry design was used to identify and document the limitations that information technology professionals experience when working in organizations that handle CUI data for the U.S. Government.

The project gathered information regarding limitations from IT individuals who work in these organizations, causing them to be unable to complete the NIST SP 800-171 requirements. Information gathered from this study worked toward closing the gap by identifying these limitations, which allows organizations to understand them and helps address them when implementing NIST SP 800-171 requirements.

1.3.2 Project Question

PQ1: What are the implementation limitations IT professionals must resolve for NIST SP 800-171 compliance?

1.3.3 Project Justification

Organizations are unaware of what limitations exist when implementing the NIST SP 800-171 requirements, representing a gap in practice. This gap creates a lack of compliance required by any government contractor working with government CUI data (Sera-Brynn, 2019). This study used the qualitative inquiry method to address limitations that IT professionals are working with when implementing the NIST SP 800-171 requirements.

The semi-structured interviews of professionals provided information from the information technology field and were able to share their expertise when working with the NIST SP 800-171 and to share what conditions exist that limited their ability to realize successful implementation. This approach addressed ideas about essential issues or aspects of the subject (Cooper et al., 2018). The study builds upon current scientific knowledge by asking these individuals about their experience in implementing and maintaining these requirements by gathering information on limitations that deter a successful implementation (Troia, 2018).

1.3.4 Project Context: Company or Industry

This capstone project explored IT professionals from the United States with experience implementing the NIST SP 800-171 in their organizations. The need to implement NIST is often based on agreements between government entities and the organization and is built into their contract (Kendall & Long, 2018.) Organizations with government contracts that maintain government data require the NIST SP 800-171 implemented to protect CUI data (Spencer, 2019). There are approximately 220,000 Defense Industrial Base (DIB) companies in the United States (Vergun, 2022). Since a high number of companies represent a large risk to government data and national security, finding ways to decrease risk has been a top priority of the cybersecurity and infrastructure security agencies (CISA, 2022). Information exists relating to the successful implementation of these requirements in these organizational types; however, the lack of information about organizations that are required to implement NIST 800-171 having the inability to implement these requirements is apparent.

1.3.5 Terms and Definitions

Terms and definitions are provided for this capstone to ensure consistency and clarity throughout the project.

Accreditation: The official authorization of a system to be operated by an approved official after validation that requirements are met (NIST, 2020a).

Baseline configuration: A baseline configuration is one where an organization can configure a system as the guideline for that system. Stakeholders should agree upon this baseline, and it should not be changed without approval (Ross et al., 2021).

Cybersecurity maturity model certification (CMMC): The CMMC was developed by NIST to replace the NIST SP 800-171 as the primary document specifying requirements to protect CUI data (OUSDAS, 2023).

Change management: Change management is a process by which an organization can purposely decide what changes to implement to their system while allowing subject matter experts the ability to weigh in on the change (Lacy & Norfolk, 2014).

Information system: An information system is any system that is used to create or store data ranging from a network to a single mobile device (Ross et al., 2021).

Information security: The practice of protecting data from unauthorized access, loss, modification, or denial (Ross et al., 2021).

National Institute of Standards and Technologies (NIST): The NIST is a government organization that works to provide standards for configuration, policies, procedures, and security (NIST, 2020e).

Network: A network is a grouping of systems allowing them to share information and resources (Ross et al., 2021).

Penetration testing: Penetration testing uses tools or expertise to attempt to access a system to test its security stance (NIST, 2020f).

Risk assessment: Risk assessment is the process in which an organization can purposely evaluate risk to their organization and decide on how they want to handle this risk (Ross et al., 2021).

Risk management: Risk management is taking action to address risks to an organization (NIST, 2020d).

Risk management framework (RMF): A risk management framework is a set of documents used to help organizations conduct risk assessments and implement risk management strategies (NIST, 2020g).

Security assurance: Security assurance is the idea that an organization feels that its risk management is effective and applies a confidence level to the implementation (National Institute of Standards and Technology, 2020c).

Security requirements: Security requirements are guidelines that an organization can use to guide the implementation of a risk management framework or other security tool (Ross et al., 2021).

Security requirement assessment: Security control assessment is reviewing an organization’s security requirements to evaluate if they are implemented or adequate in addressing the risk(s) that an organization is attempting to manage (Ross et al., 2021).

Threat: A threat is something that could potentially impact an organization’s operations (Ross et al., 2021).

Vulnerability: A vulnerability is a flaw in a system that can interact with a threat to impact an organization’s operations (Scarfone et al., 2008).

Vulnerability assessment: A vulnerability assessment is a purposeful look at an organization to find or determine its vulnerabilities or lack thereof (Scarfone et al., 2008).

1.4 Doctor of Information Technology Project Specifications

As the world has grown to rely more on information systems and their connectedness, cyber threats have become a greater threat to these systems and can pose a significant risk to their operations (Elnagdy et al., 2016). Government agencies and other organizations have worked to create various frameworks to aid these businesses in finding solutions to address these threats, including the NIST SP 800-171 document (Kenyon, 2019; NIST, 2023b; Ross et al., 2021). One way that organizations can, and many are required to, protect CUI is through the use of the NIST SP 800-171 requirements (Ross et al., 2021).

1.4.1 Importance of the Project

Finding limitations that organizations face in successfully implementing the NIST SP 800-171 requirements is important because it can inform ways to secure the nation’s data and better protect it from unauthorized access. Finding a minimum level of security or baseline is paramount to our nation’s interests due to the overall increase in security afforded (Microsoft, 2018). As mentioned in this document, government contractors often represent a weak link in the security chain, creating areas where bad actors can gain access more easily than trying to gain it directly from often more secure government organizations. One benefit of the NIST SP 800-171 is that any organization can use it to provide a minimum level of data security, but government contracting policies make this a requirement for organizations that may handle CUI data prior to awarding the contract (Spencer, 2019). As with any endeavor, there are difficulties when trying to fix problems that need to be better understood, and the lack of understanding of why organizations are struggling with the NIST SP 800-171 is one of these areas (Brook, 2018).

This project can give decision-makers in organizations implementing the NIST SP 800-171 the knowledge needed to better understand what limitations exist when implementing the NIST SP 800-171 requirements (Marin, 2021). After reviewing the available literature surrounding limitations in implementing the NIST SP 800-171, it becomes apparent that there needs to be more leadership and professional practitioners' perspectives and understanding. Using semi-structured interviews to discuss these items with professionals in the field helped to gather these perspectives and provide insight to other professionals to attempt to find a way to understand these issues.

1.4.2 Approach for the Project

Information was gathered from the literature reviews below, and the information was used to determine what gaps may exist in the field that have not been previously addressed in other areas. Questions were developed from the knowledge gained during the literature review and were used in the qualitative interview process conducted for this project. There was a gap in knowledge as to why the NIST SP 800-171 requirements remain incomplete in the industry (Sera-Brynn, 2020). Determining what limitations exist that are causing the requirements not to be fully implemented can inform leadership, creating a path for leaders to creatively solve these limitations and achieve a more robust security posture (Lynch, 2020).

To create a list of limitations, I conducted semi-structured interviews, captured professionals' unique perspectives, and determined implementation limitations that can be shared. I used Zoom to interact with participants due to the functionality of reaching anyone anywhere in the country. Participants were gathered using the User Interviews, Inc. tool. To ensure that participants met the criteria, they were validated by asking if they felt they met these requirements. Limitations gathered through these interviews can be shared with others to help educate and solve reoccurring themes relating to the inability to implement the NIST requirements fully. The audio was captured and then transcribed into text format, and each participant was sent their own transcription to review to validate that what they wanted to say was captured. These transcriptions were then used to provide data that was then analyzed to determine limitations for these organizations.

Thematic analysis was completed on data captured from interview participants (Maguire & Delahunt, 2017). Once the interviews were completed, transcription was completed to ensure accurate data was gathered. The transcribed documents were organized, coded, and analyzed using Dedoose, where themes were created based on similar responses provided by the participants (Braun & Clarke, 2006). Dedoose additionally ensured that any insights gathered from the data became known and that the best information possible was gathered to determine the limitations in implementing the NIST SP 800-171 (John & Johnson, 2004). Past research in similar studies has used the Unified Theory of Acceptance and Use of Technology (UTAUT) model, including Kiriakou (2012), who used it to evaluate another NIST framework, which closely aligns with this study, making it an ideal orientation. The framework in Figure 1 was used along with the UTAUT to help me with my analysis (Venkatesh et al., 2016).

Barriers that may exist in the data collection would be participants' inability or unwillingness to answer questions concerning security within their organizations (Schwartz, 2021). These types of concerns are common among security professionals. Concerns are often solved using anonymity built into this study to ensure that participants can feel at ease about sharing and that good data results from the interview process.

1.5 Summary

Organizations have a legal, ethical, and financial responsibility to protect sensitive data in their information system. Organizations can ensure that they realize their responsibility by following best practices or other guidance to aid them in securing these information systems. One such framework that these organizations can use to secure their systems is the NIST SP 800-171; however, apparent difficulties seem to exist due to the high number of organizations that have not successfully implemented these requirements (Sera-Brynn, 2020). Finding out what these limitations are is the first step in creating a plan to address these limitations and further complete these requirements to ensure that information systems are secure and that businesses are doing their part in protecting sensitive data. This project was an industry-based project that spanned organizations that have a requirement to fulfill NIST SP 800-171 requirements. This project addressed what practitioners perceive to be the limitations to successful implementation. Section 2 includes information relating to the literature review used to derive these apparent limitations and shows where information is missing, making it difficult for decision-makers and practitioners to find ways to fully meet NIST 800-171 requirements. Section 3 comprises the project’s results, including the practitioner’s semi-structured interviews and a summary of perceptions from the practitioners in the field.

SECTION 2. LITERATURE REVIEW AND PROJECT PLAN

2.1 Introduction

Information was gathered from experts in the field to determine the limitations non-government organizations face in implementing the NIST SP 800-171 framework and building upon knowledge acquired in previous studies using a qualitative inquiry methodology. The information can then be used to determine how these limitations affect their ability to implement NIST SP 800-171 requirements and find solutions to solve them. Finding solutions to these limitations allows organizations to better secure the data belonging to the government and their own data as a secondary benefit, thus raising the industry’s security posture.

Government agencies have been working on solutions to aid industry leaders with the daunting task of protecting government information without a significant impact on these private businesses (OUSDAS, 2023). For nearly a decade, these organizations have been changing, updating, and modifying their processes to overcome the unique problem of trying to have the best option for security at the lowest cost possible (Ross et al., 2021). Information has been gathered from various articles, research documents, journals, and government documents created throughout the process, and new literature is released frequently. The government attempted to address this from the top down by signing Executive Order 13556, requiring a standardized and secure way of handling CUI (National Archives and Records Administration, 2010).

The following information shows various attempts that have been made to help organizations find ways to protect their data, showing a need for this study to determine what limitations exist in these organizations implementing these products. Version 1 of the NIST SP

800-171 document was created in June 2015, establishing a framework that organizations must use to secure government CUI data on their information systems, which allowed organizations to check compliance, report findings, and attest to meeting these requirements (Ross et al., 2021). The NIST SP 800-171 requirements allow organizations to find and report their own weaknesses in implementation and use a plan of action and milestones (POA&M) to communicate when these items would be mitigated. Organizations having the ability to then report on their level of implementation of these requirements explains why a study was needed to identify existing limitations in NIST SP 800-171 requirements implementation (Sera-Brynn, 2019).

The government often requires standards such as the NIST SP 800-171 that can be difficult for organizations to follow (Kiriakou, 2012). Organizations have been unable to address all of the NIST SP 800-171 requirements, as has been captured by various reports (Sera-Brynn, 2020). The inability to comply with these standards can lead to a company becoming less competitive when bidding for contracts or becoming the weak link in the chain of security that is critical for our current global environment. To combat the balance of cost and security, the NIST has created guides to help businesses become minimally compliant. One such guide is the NIST's Special Publication 800-171, with the first version of the SP 800-171 completed in April 2015, with a required compliance date of December 31, 2017 (Ross et al., 2021). Since these documents have been available for years, finding out why these items have not been implemented is essential. Finding what limitations exist for organizations through this study can help organizations identify why, after a considerable amount of time, they have been unable to implement these requirements.

Cybercrime has continually been rising, and the increase in risk has created a situation where organizations must keep up by increasing their security requirements (Purplesec, 2022).

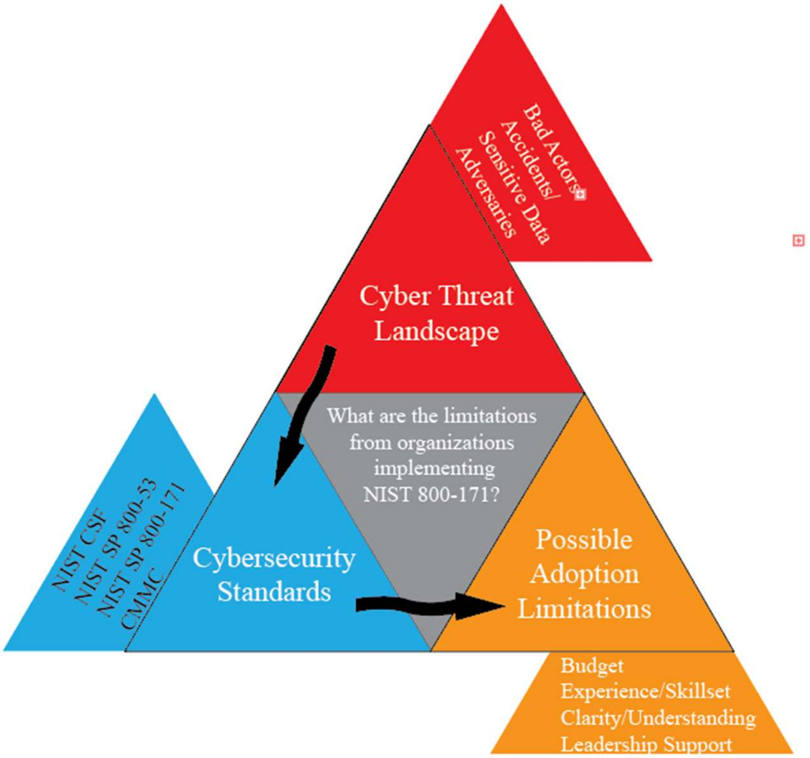
One example of how the government has tried to keep up with these threats is through updating documentation, like the NIST SP 800-181 and the recent release of the CMMC. The CMMC is a logical next step in the NIST SP 800-171 process, where organizations have an outside auditor validate the company's compliance with NIST standards, including ones in the 800-171, and new ones added to address new threats. Additionally, the ability to create a POA&M document and validate compliance is no longer accepted as a way for the Government to try and encourage organizations to implement the NIST SP 800-171 requirements fully. As Government organizations have a history of trying approaches like this, the lack of implementation by non-government organizations shows that a study needs to be completed to uncover what limitations exist (Sera-Brynn, 2019). These limitations can then inform the government and non-government organizations of ways to overcome these limitations.

2.1.1 Applied Framework

This study gathered information on how organizations accept new technologies, specifically cybersecurity frameworks and, more specifically, the NIST SP 800-171. Prior similar studies used the technology acceptance model (TAM) to gather similar information. This model uses metrics based on how useful technology is, which does not relate to this study (Davis et al., 1989; Venkatesh, 2000). Other models have been produced that fit this study better. A similar model, UTAUT, has been found in other studies that closely resemble this study, and the UTAUT model appears to be a closer match to the framework used in this study (Yvon, 2020). Using the UTAUT model as a baseline, I adapted it below to include slight modifications to address the concepts of this study directly and to ensure that the correct data was collected. The UTAUT model also aligns well with organizations attempting to implement the NIST SP 800-171 specifically and not a broad group of cybersecurity frameworks as identified by Yvon. The following framework was used while gathering limitations from IT professionals at organizations implementing NIST SP 800-171 requirements (see Figure 1).

Figure 1

Applied Framework



Note: The project author created this figure.

Figure 1 describes the intricate relationship between the different cybersecurity tools and frameworks available to practitioners today. The main question of the limitations of organizations implementing NIST SP 800-171 has various inputs representing an answer. Various frameworks have been created to address organizational risks, some of which have been derived from others. Some intend to overlap or work together to solve complex security concepts (Simplilearn, 2022). Subsequently, the cybersecurity threat landscape is so large, and the solutions to these threats are so numerous that the industry has found that the landscape has been continually becoming more dangerous and is more confused about where to start to solve these problems. When addressing today's cybersecurity threat landscape, it can be overwhelming how many threats are prevalent in the field and how often these threats attempt to act (Verizon, 2022).

As cyber threats continue to rise, bad actors have worked to find ways around security systems, and even governments are trying to attack unsuspecting victims (LeWinter, 2019). Threats range from advanced persistent threats (APT) attempting to use technology to gain an advantage against businesses and against our nation and its defenders to other bad actors that may just be attempting to hold businesses for ransom to gain monetary compensation (Tuttle, 2021).

The loss of government data is costly, and there needs to be a way of protecting these data (Reed, 2022). Frameworks outline specific actions an organization should take to secure various vulnerabilities to deny the bad actors access to information. Due to a heightened threat landscape, organizations have attempted to find ways to solve these threats, ranging from digital tools such as firewalls to creating policies and procedures such as laws or regulations.

One type of tool is the cybersecurity framework. Organizations have struggled to find a way to balance their security to best protect against these threats without breaking the bank or without implementing security that impedes their ability to do business (Aljumaili, 2018). One way to help these organizations is through publishing best practices or frameworks organizations can implement (Cisternelli, 2022). While these frameworks have been developed to aid organizations in managing their cybersecurity stance, the fact remains that these organizations do not seem to be improving their stance (Clapper et al., 2017). With a continued increase in risk, organizations are increasingly in danger of attacks; the concept that an organization is too small to be noticed no longer applies today (Tryon, 2018; Vistage, 2018).

One way that organizations are attempting to address these threats is through the use of best practices. One best practice used in the field for years is the NIST SP 800-171. This study looked at the NIST SP 800-171 as it applies directly to SMBs required to maintain government-controlled unclassified data (Ross et al., 2021).

The NIST SP 800-171 document was created by taking parts from a more extensive list of requirements maintained in the NIST SP 800-53 that Government agencies in the United States (NIST, 2020b). Issues with the NIST SP 800-171 have been addressed as far back as 2012, when the original version was released and still continue to be addressed, as evidenced by the creation and release of the CMMC (OUSDAS, 2023). Although there have been various renditions of the NIST SP 800-171 since then, there has seemed to be a problem based on statistics of successful implementation gathered by various organizations. One such report was provided to the president, Donald Trump, stating that agencies required more funding; at the same time, others felt that there needed to be CUI training completed to be successful in their implementation (U.S. Information Security Oversight Office, 2018).

The NIST SP 800-171 framework has been found to have implementation limitations, as noted by a yearly report created by an organization called Sera-Brynn (2019). The ability of non-government organizations to then implement the requirements of government organizations seems to be affected by these factors, as noted by Sera-Brynn in a report noting that external assessors have found that out of the companies surveyed, zero were 100% compliant, and on average only met about 39% of the NIST 800-171 requirements (Sera-Brynn, 2020).

Various government and private groups have worked to determine the importance of these requirements being followed and have modified their requirements to make these security tools more manageable and more cost-effective for organizations while still trying to balance the security required to protect data in an increasingly dangerous digital space (Myauo, 2016). Reviewing each of the changes to the NIST SP 800-171 as it has moved through revisions shows that there have been multiple attempts to tailor these documents in a way to encourage companies to follow them and even allow for organizations to *self-attest* that the organization is following these rules (Ross et al., 2021). Laws and contractual obligations have been created to make following the NIST SP 800-171 a minimum requirement should an organization want to have a contract with any part of the government (OUSDAS, 2023). While the requirement to follow the NIST SP 800-171 has been in place since 2012, companies have not successfully implemented all requirements (Sera-Brynn, 2019). With these laws in place and contractual obligations, non-government organizations who have a contract to handle CUI have a requisite to follow the NIST SP 800-171; however, these organizations are not following these requirements, which highlights a need to find out why these requirements are not being implemented. This study gathered information from experts in the field to understand experts' sentiments as to what implementation limitations they have and thus close the gap of requirements not being followed.

When reviewing the previous information and looking at the lack of success that organizations have had in implementing these frameworks, even with a requirement to do so, it becomes apparent that there must be something underlying as to why it has not happened (Granneman, 2019). Organizations often decide it may be better to implement a risk transference policy, such as employing cybersecurity insurance (Hiscox, 2022). While the insurance tactic has worked in the past, the increasing number of breaches has caused insurance companies to rethink their strategies and require minimum cybersecurity requirements that are just like their own frameworks, making it much more difficult for organizations to acquire this type of insurance (Violino, 2022).

In this study, I asked professionals about their experience implementing the NIST SP 800-171 requirements and discovered items limiting their ability to implement them fully. While research has been completed by others to look at other NIST frameworks and determine what is impeding them (Kiriakou, 2012), my study extended this knowledge by looking at the NIST SP 800-171 requirements specifically.

Determining why organizations may choose one cybersecurity framework over another could add to the body of knowledge (Troia, 2018). Studying the implementation of NIST requirements and finding limitations, as represented in the possible adoption limitations portion of Figure 1, can be gathered and shared. Knowing the limitations helps organizations address them and improve the body of knowledge while helping businesses better secure their networks (Complyup, 2022). Addressing these limitations may aid government agencies in finding ways to help businesses implement their requirements.

2.2 Method for Discovering Literature

Literature has been reviewed from various sources to evaluate government compliance requirements, how organizations working with the U.S. Government implement these requirements, and implementation success information. My literature review comprised multiple phases of information gathering. The information gathered began with a review of government regulations and documents, as well as laws and executive orders. Next, in the process, I reviewed academic sources such as journals, articles, studies, and other written documents. Finally, online sources were used, such as industry websites, research, and reports.

2.2.1 Inclusion and Exclusion Criteria

Selecting and evaluating articles was based on using scholarly or business articles from trusted sources. The criteria continued to include materials that relate to the NIST SP 800-171 directly and was expanded to include the CMMC model as a future replacement for the 800-171. The CMMC model was included because it includes the same requirements as the current 800-171 document and, in the future, will be the replacement for the NIST SP 800-171. Additionally, other documents, articles, and books were included to help orient the conversation around NIST SP 800-171 requirements, enabling the layperson to understand them and highlight the experiences government-related organizations have had in implementing these requirements and implementation metrics captured by professional researchers in the field. Documents were selected on their relevance to the study's goals of finding limitations.

Exclusion criteria come primarily through publishing dates to ensure that articles are not outdated or superseded. Secondarily, articles contained in non-scholarly locations were not used.

2.2.2 Search Strategy

Discovering literature for this study consisted of using literature gathered from educational documentation, government documents such as the NIST SP 800-171, related documentation found in Summon, and online sources. These documents were primarily limited to recent professional documents, scholarly articles, and peer-reviewed documents. In some cases, older documents were used to establish a link between older information and current information in the field. Search terms were primarily NIST, NIST SP 800-171, CMMC, and NIST CSF.

Beginning with a search of Summon and other online libraries, information gathering began by looking for a gap in the literature concerning various cybersecurity concepts. Over time, it became apparent that there was a gap in the literature relating to the limitations of organizations implementing NIST SP 800-171 requirements. Once a gap was found, I expanded my literature review to include searching using other online sources such as Google Scholar, business websites, government websites, and others. To ensure that research into the topic was complete, multiple search terms were used relating to NIST documents as well as the CMMC model and other cybersecurity frameworks. The search tools above yielded a vast amount of information from sources such as publications, peer-reviewed journal articles, government documents, regulations, requirements, laws, and even books. These sources were used to assess this study's concepts and create definitions listed previously in this document, as well as to establish the requirements for this study.

2.3 Review of Scholarly and Practitioner Literature

Literature has been reviewed from various sources to evaluate what government compliance requirements exist, how organizations working with the U.S. Government implement these requirements, and how successful organizations are with these implementations. The literature review in Section 2 draws from scholarly articles, government documents such as laws and regulations, professional journals, books, websites, reports, scholarly research, and case studies.

Chapter 2 focuses on the overview of requirements for CUI, as well as the reasons for updating these requirements. The chapter then transitions into how organizations have been implementing these requirements and the success of these implementations.

2.3.1 Historic and Current Business Technical Problem Trends

Problem trends in the IT field can be summarized by understanding how and why the requirements were created, how specific organizations attempted to address these requirements, and finally, through information captured in the field about how successful these attempts were. This section starts by defining the requirements and why the NIST SP 800-171 is required, continues showing an official audit of small businesses in the missile defense area, an attempt to outsource these requirements, and finally, complications that have been reported in implementing the NIST SP 800-171 requirements.

2.3.1.1 *Controlled Unclassified Information (CUI) Requirements*

A chain of conditions, beginning with the President of the United States, creates a requirement for organizations to implement specific security measures. One such legal requirement of these organizations is implementing a CUI protection program by following NIST SP 800-171 and CMMC requirements. Complexity exists in determining how these requirements interact with organizations; following a chain of requirements starting from the top is the only way to determine whether an organization must follow NIST requirements. The chain is structured so that each requirement builds upon the last. An ideology frequently used in government documentation is called *nesting*. The first and highest of these documents is Executive Order 13556, which directs organizations to protect CUI. From here, the FAR and then DFARS documents were created to support this executive order, extended the requirement to safeguard *covered defense information,* and added the obligation to report cyber incidents involving government data, among other things (NASA, GSA, & DOD, Federal Acquisition Regulation1-1-53-1, 2022; DFARS, 2020; Federal Register, 2020). The 252.204-7012 document states that "The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017" (FAR, 2023, para. 19). Mitigating circumstances impedes small businesses' compliance with CUI requirements (Patterson, 2017). A lack of security relates to the ability to protect government data from attacks. With each change to the CUI protection requirements, private businesses can keenly feel the impact of these changes, which can be highly detrimental to small businesses. However, these requirements are critical to the security of the United States, and the government must continually evolve and adapt its directives to meet the threats imposed by bad actors.

Due to an inability, or possibly lack of desire, to implement the security requirements required by these directives, the government has had to evaluate its approach (OUSDAS, 2023). The new approach was the recently released CMMC guidance, which requires an outside audit to be completed for any contractor that wants to have a contract enabling them to work with the DoD. Organizations are working toward getting certified as a CMMC Third-Party Assessor Organization (C3PAO) (CMMC Accreditation Body, n.d.) The C3PAO would then provide services to assess organizations and certify that they are appropriately following the requirements and protecting CUI. Implementing the CMMC, training C3PAO, and creating infrastructure to support a new process will take time. However, in the meantime, government-related organizations are working on finding ways to update their compliance programs from the 800-171 to the new CMMC. One should note that the SP 800-171 is still undergoing changes, and in February 2020, the NIST released Revision 2 with an update to it as recently as January 2021 (Ross et al., 2021).

The new CUI requirements represent some initial and continual costs to organizations wishing to do business with the government and continue to be confusing to government-related organizations (Jefcoat et al., 2018). Reports suggest that CUI data are still not being protected and that organizations are not compliant with the requirements of the NIST (Doubleday, 2018). One of the most significant changes in the cybersecurity field has been the new focus on the supply chain to include small businesses. Small companies typically do not have large IT staff and can be vulnerable to attack, representing a point where attackers can get into the chain (Patterson, 2017).

The U.S. Government attempted to determine what effect the CUI programs have on small businesses, finding that organizations have foundational items that must be met. One such foundational item is that all CUI needs to be located, and the systems that maintain this information must be identified. Next, a Program Management (PM) Office needs to be developed or someone appointed to follow the CUI data and ensure it is properly handled. A policy also needs to be created that outlines the procedures used to protect the CUI in the program. As with nearly all programs, the development of training is critical, including topics like computer security, PII, and insider threats. Finally, there is a need to develop a program that includes self-inspection tools and appoint someone to manage the program (U.S. Information Security Oversight Office, 2018).

There have been reports in the past identifying problems with the compliance of small businesses. The ability to meet the requirements and self-attest has left room for negative results, which has caused the Federal Government to determine that there is a lack of oversight into these programs, which is partially why the C3PAO requirement has been created (U.S. Government Accountability Office, 2017). The U.S. Government then decided that regularly scheduled outside validation is required to ensure compliance, which seems to be supported by the evidence below. In addition, there was an implication that the program was expensive, created a burden and that the time established for companies to prepare for implementation of these requirements was not used, and companies were scrambling to become compliant once the deadline was reached (U.S. Information Security Oversight Office, 2018). Further information comes from the article *Assessing the State of a Contractor's Internal Information System in a Procurement Action* (Hawes, 2018).

2.3.1.2 *Missile Defense Small Business Audit*

The Inspector-General of the U.S. Department of Defense conducted an audit of the Missile Defense Agency (MDA), which acts as a sponsor for contractors. During the audit, it was found that security requirements were not consistently implemented across organizations, supporting the idea that there are issues with the ability to implement the NIST requirements as in 2018 (U.S. Department of Defense Inspector General, 2018).

The U.S. Information Security Oversight Office (2018), along with the Executive office, provided guidance to contractors through the use of the *CUI Notice 2016-01, Implementation Guidance for the Controlled Classified Program*. One hundred thirty-six government agencies were contacted and directed to implement the CUI program by September 2017. However, two years later, it was still not complete (Lynch, 2020). Many organizations view the CUI program as burdensome, expensive, and not important enough to include in the budget (Troia, 2018).

One way that the government has attempted to add strength to the requirements to follow these requirements is through the process of gaining contracts (Kendall & Long, 2018). Sponsor organizations are required to determine if the contractor can protect CUI, but there was no way to ensure businesses had buy-in. Meeting the requirements before a contract award can motivate organizations to follow these requirements (U.S. Department of Defense Inspector General, 2018).

The document *Assessing the State of a Contractor's Internal Information System in a Procurement Action* requires defense contractors to provide contracting officers proof of CUI implementation before new or future award of contracts (Federal Register, 2018). Still, it seems that the process did not quite meet the needs. Since the new CMMC model has required that the certification level of a contractor be provided before contract award, government-related contractors are now, for the first time, having to spend time and money on this level of security before receiving funds from the government (OUSDAS, 2023). In late 2020, an interim rule was created that required contractors to report their compliance level in the Supplier Performance Risk System (SPRS), among other requirements (DFARS, 2020).

The U.S. Government decided that to manage the implementation of the NIST SP 800-171, they would write the directive into the contract (Kendall & Long, 2018). Future awards of contracts can also encourage organizations to follow the guidelines. Furthermore, the U.S. government requires documented proof of CUI compliance after the contract is awarded (Kendall & Long, 2018).

Small businesses often outsource IT and cybersecurity personnel due to their inability to hire a large enough IT staff to meet the requirements leveraged by the NIST requirements (Nichols-Jackson, 2016). Additionally, these organizations do not perceive themselves as potential targets because of their status as small companies or because these companies are being monitored (Ramsay, 2015). Security through obscurity strategy leaves government-related organizations vulnerable to attack because security measures may be ignored since organizations may deem these measures *overboard* (Ramsay, 2015). Cybersecurity is one field where company stakeholders are critical to the process and require at least a working knowledge of their systems (Dolan, 2022). Finding and hiring staff that are skilled at implementing security has shown to be difficult, creating a large cybersecurity talent gap (Security Magazine, 2020). Organizations protecting Government data, as well as various other laws and requirements, should create an environment where at least the minimum requirements are met by small businesses; however, research has shown that this is not necessarily the case, partly due to the fact that there is a talent gap in cybersecurity professionals, which means even if a business intends to meet these goals these organizations are going to be met with limitations barring them from fully implementing these requirements (Bonnema, 2018; Brown, 2016; Ross et al., 2021).

2.3.1.3 *Outsourcing Controlled Unclassified Information Mandates*

Considering the cybersecurity talent gap and various monetary constraints, small companies may be required to outsource to handle CUI requirements. One way this is done is by sub-contracting an external entity to perform the work for an organization (Twin, 2021). When reviewing the frequency of outsourcing, it is apparent that this is common in government-related and non-government organizations and industries, and evidence shows that doing so can significantly improve an organization's security stance (Nero, 2018). These outsourced IT professionals work daily in the field and have a breadth of knowledge from working with other networks and organizations (Nero, 2018).

Outsourcing can also include the use of cloud services, which comes with another set of requirements, such as the Federal Risk and Authorization Management Program (FedRAMP) requirements. While these extra requirements can burden organizations, the requirements also allow these agencies' sponsors to award contracts and store their data securely at a lower cost than with on-premises infrastructure (FedRAMP, 2021).

2.3.1.4 *Complications with the implementation of the NIST SP 800-171*

When NIST SP 800-171 was initially released, it was done so with concerns coming from organizations as to the cost of these implementations. Companies have felt these complications since the initial release. Organizations have been having difficulty implementing many different NIST products, ranging from the Cybersecurity Framework to more specific documents such as the NIST SP 800-53 and NIST SP 800-171 (Kiriakou, 2012; Simonova, 2020; Yvon, 2020). The U.S. Government has worked hard over time to find ways to evaluate the application of its regulations, laws, or frameworks. Overall, represents a trend that the U.S. Government is always looking for more insight into what is happening within and without. As mentioned previously, in the area of the NIST SP 800-171, government agencies ranging from the office of the president through the contracting office, all the way down to the NIST, have been iterating through the protection of CUI in various ways. One way is through the iterations of the NIST SP 800-171 framework, which has been historically used to help government contracts set up a minimum standard of security that can protect government data when working with a government customer.

Since NIST SP 800-171 was released in 2012, research has been conducted by various agencies and companies to determine its effectiveness, which has shown that once the research is complete, it often results in a modification of the NIST SP 800-171 standards and a re-release of these standards as supersession to the previous version of the document (Edwards, 2017). In the past, it has been attempted to find the common deficiencies between organizations to determine a way to address them, but it does not seem to have had any effect on an organization's ability to successfully implement them (Sera-Brynn, 2020; Sundararajan et al., 2022). Finding common deficiencies has not solved the problem relating to companies' inability or unwillingness to implement the requirements fully. Instead of finding out which difficult items are not being implemented, this study intends to find out from professionals in the field what limitations exist, causing them not to be able to implement these requirements.

2.3.2 Previous Efforts to Address the Problem

NIST has worked for years through iterations to attempt to address the fact that organizations have not been able to successfully implement the NIST SP 800-171 through reports, and even though requests for comments that can be implemented in future versions of the document (NIST, 2023a; Sera-Brynn, 2019). By modifying the NIST SP 800-171 program either directly through the document or by structuring requirements around the document, such as changing the contracting vehicle or requiring third-party assessments. Additionally, a site has been created to track updates of the NIST SP 800-171 document to address these comments (NIST, 2023b). The combination of the history of audits and reports and the various attempts to address the lack of 100% compliance with little to no improvement shows limitations for organizations attempting to meet these requirements (U.S. Department of Defense Inspector General, 2018). The most recent attempt to address the problem was by creating and implementing the CMMC model, which requires third-party assessments to include a new pass/fail scenario. This requirement was created because organizations were writing POA&Ms to avoid having to implement various requirements (Noonan, 2022). The requirement shows that instead of solving the implementation limitations. The government is attempting to force companies to comply through legal means and thus performing a risk transference from the loss of data risk to one of blame if organizations do not protect government data successfully.

2.4 Summary of Literature

Due to the connectedness of our society and the fast changes inherent to technology, organizations need to improve security continuously, implement a minimum baseline, and find creative ways to do so to be able to afford the security required to protect themselves and the government (Reed, 2022). The NIST 800-171 requirements represent a great start at security, and these requirements can be considered a minimum requirement to protect data (Harrington, 2022).

Organizations should strive to meet the minimum and find ways to do so with limited budget, time, and experience emphasized as a priority. My research attempted to find limitations that organizations are experiencing in implementing these requirements and should help to add to knowledge on how to fix these limitations to enable the organizations to meet these minimum requirements, improving cybersecurity for the entire field.

2.5 Recruitment

Recruitment for this project was composed of current professionals in the field who must implement NIST SP 800-171 requirements in their organization, primarily made up of government contractors. This group of individuals provides the best insight into organizations' limitations in their ability to meet the NIST provisions because the experts have experienced firsthand what is required to implement them.

These individuals came from IT departments or offices in their organization and had at least one year of experience in the IT field to ensure that the respondents were experienced in IT and had the knowledge required to comment on the limitations in implementation and were not made up of inexperienced professionals.

Respondents were found using User Interviews, Inc., leveraging their built-in recruitment tools and professionals included in their products. Using User Interviews, Inc. allowed me to use their expertise in finding participants, ensuring that each participant matched the recruitment standards required for this study, and providing a platform for interaction with the participants, including sharing documentation. Since all of the respondents had experience in working with the NIST SP 800-171 document, participants were selected randomly through User Interviews, Inc. until 12 were reached, ensuring that there was an appropriate number of interviews conducted for an appropriate data collection.

2.6 Project Study Protocol

The purpose of this study was to gather information relating to identifying NIST SP 800-171 implementation limitations for government contractors. A previous review of current literature has found various areas where many other cybersecurity frameworks were evaluated, but NIST 800-171 has so far not been included in this evaluation. The NIST SP 800-171 specifically is used to protect CUI in non-government organizations, which is imperative because these supply chain organizations represent the biggest threat to government data loss (Pabrai, 2022).

This study gathered information that can be used to target the limitations they are experiencing and thereby work to solve them. Participant confidentiality was of utmost concern during the process, as sharing limitations with an organization's information system can often be sensitive. Confidentiality ensured an environment where the participants could answer honestly and without fear of retribution. I ensured during the interviews that the participant was comfortable by verbal verification since they participated in the interview virtually, and I did not have access to the physical environment.

2.6.1 Data Sources

To collect data from the 12 selected participants, I used a qualitative inquiry process and asked questions of the participants in interviews through Zoom.

2.6.1.1 *Preliminary Sources of Data Expected*

While completing this study, I used a variety of data sources to include a review of current documentation, including scholarly and practitioner-published articles, online data sources, and governmental documents. I also included collection data from virtual semi-structured interviews that were captured using Zoom and transcribed into a document to validate the experiences of the practitioners in the field.

2.6.1.2 *Instrumentation and Data Collection Tools*

As part of a qualitative inquiry, the instrument for evaluating the data was me. I used my impartial judgment to review all the data collected during the interview process that has been transcribed. Rev.com is a transcription website that was used to upload audio files professionally transcribed by their employees. These transcribed documents were used to categorize the answers into broad categories based on the similarity of answers. User Interviews, Inc. maintains a site that provides researchers with a platform to conduct interviews and interact with participants and was used to gather participants. I provided User Interviews, Inc. with the list of inclusion and exclusion criteria. Once User Interviews, Inc. provides a list of participants. As the instrument, I went through the list and ensured that all the suggested participants met the inclusion criteria. Next, I used the User Interviews, Inc. tool to communicate with the participants and scheduled an invite to join me on a Zoom call, at which time I conducted the interview using an audio-only recording. Once the recording was captured, I took each file and uploaded it to rev.com for transcription to a Word document. Finally, I uploaded all transcribed documents and notes to Dedoose to code the interviews and visualize and publish the data for this capstone.

I created the interview guide to aid in the interview process and ensure that each participant received the same questions. As part of our requirement to test our interview process prior to actual data collection, I used my interview guide as well as the other tools listed above to interview expert IT professionals in the field and evaluate if the questions were easy to understand and if they would capture the data needed for the study. With feedback from the test, I updated my guide to ensure it was complete.

2.6.2 Data Collection

Data was collected using the interview process captured above through audio recordings of Zoom meetings between myself and each participant. These recordings were used to document the participants' questions and answers. The participants were asked a list of the same open-ended questions and were asked each question in the same way. If questions were not answered completely or the participant did not understand the question, I asked them to elaborate, or I would re-ask the question as I did not want to change the question intent and thus cause incorrect data collection. All questions used in the interview have already been reviewed using the expert panel review process required by Capella. All the interviews were entirely recorded and submitted in their complete form. Using the rev.com transcription service, I provided all the audio captured through the audio recordings on Zoom during the interviews. This organization protected participant anonymity in two ways. First, I asked all interview participants not to share any personal information, including their information of former and current employers or other identifiable information. Additionally, Rev.com provides a privacy policy that can be found on their site, stating that they honor the privacy of all data that is received into their system. Rev.com transcribed the audio from the recording to a Word document to return to me as the instrument. After I reviewed the transcribed document for accuracy, each interview was broken into a separate document and sent to the participant who provided the interview for their review. I asked the participants to review their documents to ensure that the information contained was what they intended to convey and that it was accurate and complete. These documents were used to find themes within the information to determine which limitations exist in the participant's organizations. These themes were determined by me as the data evaluation tool and were broken into categories based on frequency and similarity. The frequency of these themes was listed to understand how often a certain limitation are noted by the participant and helped to determine which items are the most limiting to companies required to adhere to the NIST requirements.

These limitations are shared in Section 3 in tables that show the frequency in which these limitations were mentioned by the participants and sorted with the highest number at the top and the lowest at the bottom. Sorting helps to determine the most impactful limitations due to the frequency with which various organizations notice these limitations. The tables provide a quick view to readers of what limitations are the most widely felt by the professionals in the field. Limitations listed at or near the bottom of the table are rare and may represent limitations that most practitioners may have already solved in their environment. Knowing the number of limitations and the frequency in which the limitations appear can be used to prioritize the list of limitations for other researchers to determine the next step in working through them with organizations.

2.6.3 Data Analysis Plan and Presentation

The overall objective of data analysis was to answer the project question. Once data were collected from the interview process and transcribed from the Zoom interviews into Word documents, transcriptions from the interviews were uploaded into Dedoose (Dedoose, n.d.). Using myself as a tool, Dedoose was used to employ the thematic analysis procedure to identify themes in the responses, which was critical due to the amount of data that was gathered in the interviews (Dedoose, n.d.). Thematic analysis was completed using steps created by Maguire and

Delahunt (2017). Using Dedoose, I generated initial codes to categorize the data. Using a theoretical thematic analysis, I used the codes to capture data relevant to the research question.

Once coding was completed, I used the codes to find themes in the data. Calling upon knowledge gained by working more than 25 years in the field, a review of the themes was completed, and all relevant data were gathered and attached to these themes. These themes were then used to list the limitations that IT professionals see when implementing the NIST SP 800-171 and can further be sorted to determine the most widespread or the least frequent. Themes were defined in preparation for the final write-up. The write-up was developed to specifically speak to IT professionals who have a requirement to implement NIST SP 800-171 and can benefit from knowing these limitations. This write-up includes the outcomes found in the study, the findings, and the list of limitations as possible recommendations for the audience.

Data are presented in a list of limitations formatted from the most frequently occurring to the least frequently occurring. Similar terms were combined during the categorization of the data into themes to ensure that the data set remains small and easily digestible. For example, if a participant responds, “I do not know how to do this requirement,” and another responds, “I have never been trained to do this requirement,” that can be summarized as a “lack of knowledge in implementing this requirement.” Any data that deviates from the themes found in the original data set was left out to ensure that the question regarding limitations in implementation was the only question being answered.

2.6.4 Trustworthiness

Lincoln and Guba (1985) were the first to identify credibility, dependability, confirmability, and transferability and guided in designing studies that relate to gathering information through their Naturalistic Inquiry system. Using these criteria, one can take an objective look at the gathering and interpreting of data to ensure overall trustworthiness in the information (NCU, n.d.).

In this study, credibility was established by vetting the participants to ensure appropriate knowledge of the topic and experience in the area of study and through sharing of experience (Cope, 2014). Credibility was an important factor for this study due to the importance of understanding why an organization would choose to or not implement the NIST SP 800-171, which is a primary concern of the entire study, and providing prolonged engagement will improve credibility (Korstjens & Moser, 2017).

Once the information was gathered, it was essential to ensure that the data was dependable, meaning that the data remained the same and was not changed throughout the study and that what the respondents wanted to say was conveyed and understood. Ensuring that the research steps are recorded ensures dependability as well (Korstjens & Moser, 2017). Two items were used to ensure dependability, first using the record and then transcribing to ensure that the data created was immutable. Additionally, this transcript was sent to the participants to review and validate that it accurately captured what was intended, ensuring dependability, as noted by Cope (2014).

Confirmability was used to ensure that there was no bias included in the data as it was gathered through transcription and validation with the participant and using a coding schema to identify patterns scientifically without researcher bias. As linguistic creatures, all human research is conversational, and asking open-ended questions further allows the participants to share their experiences (Brinkmann, 2012). Combining these questions with the coding ensured that bias did not seep into the process as much as possible. The transcription process and sharing of the transcript with the participants also provided confirmability (Cope, 2014).

Finally, addressing transferability was done through an interview guide that ensured that the same questions were asked to each participant, ensuring the same opportunity to share their experience. Evaluating not only the research process and the interview process, but a thick description was also included to ensure transferability (Korstjens & Moser, 2017). Information gathered can then be used by others to further add to the research of others to perform similar studies meeting the intent of transferability (Cope, 2014).

2.6.5 Ethical Considerations

The primary ethical consideration of this study was the possible implications that a participant could have if their responses were to be shared with their employer or other outside parties. As provided by the *Belmont report*, the assessment of risks and benefits and selection of subjects was completed following these principles (United States, 1978). Participant information was captured anonymously using tools such as translating names to numbers, ensuring that participant comments cannot be associated with them in any way, and meeting the privacy and confidentiality requirements. Participants were notified of their inclusion in the interview and were asked for their approval to be interviewed (Creswell, 2014). Sharing security information about an information system is often sensitive to organizations, so ensuring that information was redacted protects these organizations and ensures that the information gathered for this study was only used to find generalized limitations for the entire field rather than an individual organization.

Capella University Institutional Review Board (IRB; Creswell, 2014) approval was obtained prior to any interactions with participants, and participants were gathered after the process was complete, ensuring that ethical subject matter experts were consulted, providing the board the ability to address the process to ensure that the highest standards were met.

2.7 Overview of the Project Study Plan

The project study timeline consisted of gathering approval from the IRB, at which time I began working with User Interviews, Inc. to capture participants for my study. Once participants were gathered, I established appointments to meet with them virtually to conduct the interview, which took approximately 45 to 60 minutes to complete with each participant. I limited interviews to 12 participants to ensure that the timeline could be quickly completed while ensuring enough data to capture the data to be fully used in the study. Once I was approved, interviews were conducted within a 2-week span to ensure that the data was relevant to the current period, as the environment is significantly changing and technology changes very quickly. Once all interviews were completed, I submitted the audio recordings to a transcription service to ensure accuracy and timeliness in transcribing the data. Upon receipt of the transcriptions, I worked to categorize the data to present in the third section of this document.

2.8 Summary and Conclusion

The purpose of this project was to identify limitations in an organization's ability to implement the NIST SP 800-171 cybersecurity framework. Current literature shows a knowledge gap that addresses this specific problem. The purpose of this study was to answer the question, "What are the implementation limitations IT professionals must resolve for NIST SP 800-171 compliance?" by completing qualitative inquiry interviews, from which the participants were pulled from a pool of organizations that are required to implement the NIST SP 800-171 requirements. The current documentation, as well as the interview answers, was used to find these limitations.

SECTION 3. RESULTS, DISCUSSION, AND IMPLICATIONS

3.1 Introduction

The qualitative inquiry used in my study aimed to explore the possible limitations that organizations encounter when implementing the NIST SP 800-171 guidelines. Gathering data from practitioners in the field was completed through interviews conducted to ask about the participant's experiences in the implementation of these guidelines. Through evaluating these experiences, the data captured supports the capstone question as it relates to possible implementation limitations IT professionals must resolve for NIST SP 800-171 compliance.

3.2 Data Collection Results

In order to fairly capture data relating to possible limitations, practitioners from the field were recruited using the online website User Interviews, Inc. to ensure that a wide range of experiences and perspectives were evaluated. Through User Interviews, Inc.'s screening questions tool, an initial opportunity for participants to self-identify as meeting the requirements for the study was completed. This screener allowed the researcher to have an initial filter of participants who did not meet the requirements to be left off of the list. Once the participants answered the screener indicating at least one year of experience in the IT field and have applied NIST SP 800-171 in their organization, the researcher further reviewed the participant's job titles, industries, and locations to create a list of participants to invite for the interview process.

Once the list was created, invitations were sent to each participant to a Zoom meeting to allow for the recording of audio that was later used to transcribe Word documents to capture the information shared by the participants. Once the participants arrived at the interview, I gave them a brief overview of what the study was for, validated that they were okay with being recorded, and further confirmed that they met the study requirements to be a participant. After the initial requirements of the meeting were met, I asked open-ended interview questions to allow each participant the ability to discuss their experiences in each area. Once all questions were asked and follow-up questions were completed, I let the participants know that I had stopped recording and let them know that I would follow up by sharing the interview transcript with them and that they would receive their incentive as a gift card. Table 1 captures the participant's demographic information below.

Table 1

Job Titles, Location, Industry

Participant	Location	Job title	Industry
1	New Jersey	Cybersecurity analyst	Computer & network security
2	Kentucky	Unix system administrator	Computer & network security
3	California	Information professional	Computer & network security
4	Massachusetts	Director of cyber security	Insurance
5	North Carolina	Information security professional	Computer & network security
6	Maryland	Cybersecurity manager	Information technology and services
7	Illinois	Vice president	Retail
8	Ohio	Product owner	Information technology and services
9	California	Network engineer	Computer & network security
10	Georgia	Network engineer/network administrator	Computer & network security
11	New York	IT help desk administrator	Computer & network security
12	Texas	Vice president	Computer software / SaaS

3.2.1 Ethical Considerations

Finding participants using User Interviews, Inc. was completed using the built-in toolset. Settings for standard demographics such as age, race, gender, and income were not used as the goal of this study was to garner participants from occupations in the IT career field. Professional characteristics were then used to include any job title as long as the participant met the requirement of at least 1 year of experience in the field and experience implementing the NIST SP 800-171. Only participants meeting the screening criteria were forwarded to the study, and all others were not included. Of the participants that were sent over, 19 were generally qualified, of which I randomly chose the first 13 that accepted entry into the study to interview to ensure that there was no internal bias when selecting candidates and providing one extra candidate should there be a complication with a participant allowing me to meet the 12 initially planned for the study. In total, 13 participants were interviewed, with one participant being removed from the study. As noted in Table 1, this process led to a good set of candidates from different areas of the country, different job industries, and different job experiences.

3.3 Data Analysis

This study used qualitative inquiry to examine limitations that organizations felt when implementing the NIST SP 800-171. The project question answered was, “What are the implementation limitations IT professionals must resolve for NIST SP 800-171 compliance?” Ensuring that a correct thematic analysis was followed, the study used the Braun and Clark analysis process (2017) to create initial codes that were created by evaluating the data gathered during the interview process. User responses were captured via Zoom audio recording and sent to rev.com for transcription. When the transcription was returned, the researcher validated it for accuracy by listening to the recordings a second time and following along with the transcription through the Rev.com built-in tool. The transcription was then forwarded to the participants for their input and approval. Each transcription was then uploaded to the Dedoose tool, which was used to create the codes based on the participant’s answers to the interview questions. The plan in previous sections was followed with only one variation of note where the participant was unable to complete the interview due to interruptions and their inability to focus on the interview. For this reason, the participant was notified that the interview would be finished and was removed from the study.

3.3.1 Initial Coding

Initial coding in Dedoose led to 60 codes captured based on wording captured in the transcriptions. Following the thematic analysis process, the researcher completed further iterations of the coding process and settled on 41 codes to be used to create themes and categories in later analysis (see Table 2).

Table 2

Initial Coding Structure

Codes	Examples	Code by occurrence count	Number of participants
Business concerns	'They look negatively on cybersecurity requirements as, oh, they are just trying to limit what we could do' (P1).	67	12
Funding	'Boils down to the budget going, to be honest' (P10).	65	12
Employee education	'The biggest thing is education for the users' (P1).	33	10
Employee attitudes	'They want to do it, but they are afraid to make a mistake and then be labeled or put on some list for the next five years' (P3).	34	10
Lack of IT Standardization	'You have to have someone or a team in place that is going to ensure that those measures are being taken care of to correct any issues' (P2).	62	10

Codes	Examples	Code by occurrence count	Number of participants
Insufficient Communication	‘Speaking their language and not having them translate it in their minds’ (P6).	20	9
Internal policies and procedures	‘Policies that are, even if they have been updated annually, are still outdated’ (P4).	31	9
Lack of IT Staff expertise	‘Hiring contractors that are capable’ (P9).	51	9
800-171 requirements difficult to understand	‘But it is usually, hey, this is requirements. We have no clue, please help’ (P10).	16	8
Interpretation	‘The way that they interpret what’s written can vary’ (P3).	23	8
Requires third-party pools	‘It could be automated, or we just do not have the tools’ (P3).	17	7
Management buy-in	‘Getting the senior leadership on board that we met obstacles there’ (P9).	29	7
Time/scheduling	‘But there are so many different requirements that we just do not have the time to do that’ (P3).	23	6
Conflicting guidance.	‘They are written with the concept of passing their SEC audits in mind, so they do not want to proclaim or say they do something wrong’ (P7).	12	5
Conflicting internal processes	‘Move too fast sometimes, and they do not do all of the proper security reviews’ (P5).	8	5
800-171 scalability difficulties	‘The blanket approach … increase the complexity within itself and the cost’ (P8).	66	4
Difficult to consume	‘Just trying to distill it down, that has been kind of a challenge’ (P3).	9	4

Codes	Examples	Code by occurrence count	Number of participants
Lack of established IT procurement process	'But a security perspective from an IT person, an IT person, if it is not broke, they do not fix it' (P12).	7	4
Management understanding	'People up top do not understand what they are paying for' (P11).	5	4
Other documents	'But it is like each time you go to another document, it might reference something else. Just keeps going down and down the rabbit hole' (P6).	5	4
External pressures	'Not be able to renew our contract' (P5).	5	3
Keeping it up	'If I have met the requirement, then I am done. No part of that met the regulation is that continual improvement' (P12).	5	3
Lack of examples	'And when it comes to implementing something that they have never done before, they need real detailed information' (P5).	8	3
800-171 insufficient	'One size fits all just does not work' (P4).	4	2
Lack of internal policies or procedures	'Well, I think in general, just not having that in place, maybe their current policy, I mean, they just have done it, and so certain policies may be implemented' (P2).	3	2
Not knowing the environment	'People do not even know what kind of data are lying where' (P8).	4	2
Partner security	'A lot of the things that people do not talk about is people have gotten security access due to contract modifications or some sort of what would be considered	4	2

Codes	Examples	Code by occurrence count	Number of participants
	business modifications' (P12).		
Resistance to change/general resistance	'People are going to rebel' (P5).	7	2
800-171 future improvements	'Draft of the revision is making it better, not worse' (P5).	1	1
Helpful external pressures	'Customers very often drive the adoption of controls' (P4).	6	1
Lack of documentation	The reality is if you go from contractor to contractor and have different contractors going through what you ought to do, having independent eyes look at things, you have to have a level of consistency with your documentation to speed up that process. (P12)	3	1
Lack of continuous improvement	'But a security perspective from an IT person, an IT person, if it is not broke, they do not fix it' (P12).	1	1
Lack of internal Written standards	'Hey, I have got a really great idea. And the next thing you know, you have now got technology running in an environment somewhere' (P7).	1	1
Lack of standardization of systems	'But I think the biggest problem that companies run into is a little thing we denote as one-offs' (P7).	2	1
Nonstandard items in the information system	'As far as number one, just what you can break and implementing security as a lot of these organizations	1	1

Codes	Examples	Code by occurrence count	Number of participants
	have a lot of home-cooked stuff' (P2).		
Security and operations job separation	'The fox watching the hen house kind of thing' (P4).	2	1
User skillsets	'Just do not have the budget to hire maybe more qualified staff' (P3).	4	1

3.3.2 Initial Categories

Categories were created by evaluating the various codes and determining which codes fall into a similar category. For example, from the codes above, Employee fear and management buy-in can both be categorized as part of the aspects of business culture. From the initial 38 codes created through the iterative process, six major categories became apparent and were built into Table 3.

Based on the information contained in the table below, when looking at the occurrence rate, it appears that the two biggest categories that lead to implementation limitations are lack of resources and aspects of business culture, showing 259 instances of resource data and 209 in culture. The same result can be found when reviewing the number of participants with similar concerns, showing 12 of 12 participants listing limitations in the culture and resources category.

Table 3

Categories

Category name	Description	Number of codes	Number of occurrences	Number of participants
Resources	Participants feel that a lack of various resources causes organizations to be limited in their implementation of the NIST guidelines.	10	262	12
Culture	Aspects of the business culture contribute to limitations in implementing guidelines.	12	209	12
Clarity	Participants believe that there can be difficulty understanding various aspects of NIST requirements.	6	86	10
Conflicting requirements	External factors such as laws, processes, customers, or partners limit an organization's ability to implement the guidelines.	12	35	9
Framework shortfalls	Participants observed that problems with the NIST SP 800-171 itself make implementation limited.	3	11	5
Information system shortfalls	Participants noted that problems with the management of the organization's IT system created situations where implementation of the NIST guidelines is limited.	3	7	3

3.3.3 Themes

During the coding and recoding process, certain themes arose that support the study's theoretical framework as well as the study question. The way these themes were developed is by taking the initial information shared by the participants and developing codes from these responses. The codes were then reviewed and reorganized multiple times and as the codes were evaluated, categories started to appear showing how some of these codes could be grouped together. Once these categories were created, the categories were then evaluated to determine if there were common threads among the data, and these common threads were then used to create the themes. These themes provide insight into the limitations that organizations are experiencing in their environment. As described by UTAUT, the adoption of technology is determined by behavioral intention (Venkatesh et al., 2016). How businesses or their employees perceive these tools, and their other behaviors, are going to determine how successful implementation will be for that organization. Through the use of this framework, the six categories in Table 4 were then transformed into three themes. The themes that were discovered during the analysis were *User Education, Ease of Enforcement, Apects of Business Culture, Clarity of Requirements, Conflicting Requirements, Framework Shortfalls, Information System Shortfalls, and Lack of Resources.*

Table 4

Themes

Theme	Definition	Instances	Categories
Lack of resources limiting implementation	This theme captures various resources such as talented employees, financial items, timelines, and others that impact the ability of the organization to implement NIST SP 800-171.	259	Lack of skilled IT staff, Lack of educated users, fatigue keeping up the framework, lack of funding, difficult-to-use or expensive third-party tools, lack of time/scheduling.

Theme	Definition	Instances	Categories
Aspects of business culture that interfere or impede implementation	Responses relating to how business culture can interact with the ability to fully implement NIST SP 800-171.	209	Lack of IT Procurement process, Employee attitudes/fear/trust, insufficient communication, internal policies and procedures, lack of record management/ documentation, lack of continuous improvement, business goals/priorities/ attitudes, lack of internal written standards, lack of internal policies or procedures, management understanding, management buy-in, resistance to change.
Clarity of requirements making implementation difficult or impossible	Encompasses responses that highlight the clarity of the NIST requirements.	82	Interpretation, 800-171 requirements difficult to understand, framework difficult to consume, unclear, lack of examples, other documents required to support.
Conflicting requirements that block or hinder implementation	Responses indicating if there are other requirements that conflict or directly hinder the implementation of the NIST SP 800-171.	35	External pressures, conflicting internal processes, conflicting guidance/regulations, external pressures that help implement partner security.
Framework shortfalls deterring implementation	Comments relating to specific shortfalls of the NIST SP 800-171.	11	800-171 improvements, 800-171 insufficient, 800-171 scalability difficulties.
Information system shortfalls creating limitations	This theme demonstrates connections between the respondents' information system and any shortfalls that may affect the implementation of	7	Lack of standardization, lack of information relating to the environmentalization.

Theme	Definition	Instances	Categories
	the NIST SP 800-171.		

3.3.3.1 *Lack of Resources*

During the analysis of the data captured in the interview process and through the use of coding and categorization, it became apparent that there are various themes that can be synthesized from the data and from how the data was shared by the participants. Reviewing the categories of the codes, it became clear that some of the categories could be further included in a theme denoted as lack of resources. This lack of resources can show up as a lack of trained IT staff, insufficient funding to purchase required technologies or even a lack of time to implement due to short timelines. Finding solutions to overcome the lack of resources is something that many organizations struggle with, and it came up through various interviews during the data collection for this project (see Table 5).

Table 5

Participant Responses Supporting Lack of Resources Theme

Theme	Examples
Lack of resources	And then the resources at the business line level, to my culture comment earlier, the business line is tasked with making money, selling products, and getting them to divert their limited resources with developers or whatever to make sure their products are secure can be a tough sell. (P4) ‘So how do you want to go about implementing something that potentially has a financial burden’ (P1)?

3.3.3.2 Aspects of *Business Culture*

One primary theme that arose when reviewing the interview data was aspects of business culture. Many aspects of business culture can create an environment where there are limitations in implementing the NIST requirements. This theme encompasses categories such as management buy-in, employee attitudes, and business requirements.Respondents discussed how security is often a secondary concern, showing that management buy-in, or even employee attitudes may not be prevalent for companies and described how this could lead to difficulties in implementing the NIST SP 800-171 due to the lack of support from leaders and other employees and users alike. Having a culture that is positive towards security, on the other hand, means that many of these limitations can be solved. Aspects of business culture has been identified as the second highest factor that limits implementation due to the ability to influence resources either positively or negatively. External factors such as government requirements, contractual obligations, winning contracts, or partners can also affect business culture and, in turn, increase or decrease limitations in implementing the NIST SP 800-171 (see Table 6).

Table 6

Participant Responses Supporting Aspects of Business Culture Theme

Theme	Examples
Aspects of business culture	‘I do not know if it is cultural or management driven, but yes, it all comes back to … What does the company place first? Security or something else’ (P5)? I do not want to say it is a lack of cooperation, but there was not an urgency on their side of the house. So, because it was not a priority on their side of the house, it did not get the attention it probably should have. It did not have the same attention from their IT department that our IT department had on it. (P9) And then someone in your marketing division goes, hey, I have gotten a really great idea. And the next thing you know, you have now got technology running in an environment somewhere, whether it is internal or externally facing, and your configuration management has been completely thrown off. (P7)

3.3.3.3 *Clarity of Requirements*

The clarity of requirements theme comes up frequently in the interview data as well. The reasoning behind this theme is that there are often grey areas in the requirements, causing implementers to feel unsure about what the requirement actually is. Further, when inspectors arrive, they may have a different idea of what the requirement means that conflicts with the implementor. Another area in which clarity can be an issue is whether or not an organization is required to follow these frameworks. Following the guidance can be difficult for organizations to follow, and without some other requirement making this clear, it can cause confusion. Some organizations feel that these requirements are simple due to their experience with other government documents in the past, showing that while this is a limitation for many organizations, it is not a limitation for all of them, according to the interview data (see Table 7).

Table 7

Participant Responses Supporting Clarity of Requirements Theme

Theme	Examples
Clarity of requirements	So, policies are generally written with the concept in mind that they, I am not saying that they deviate from the law, but they are not written with the concept of meeting a control framework in mind. They are written with the concept of passing their SEC audits in mind, so they do not want to proclaim or say they do something. (P7) ‘Am I supposed to even do this? Am I supposed to even follow this? While it might be black and white to the people who have written it, all right, might not be the one who’s reading it’ (P8). People kind of get confused. It is like, hey, do I just look at the overall, or which level do I look at? If I am someone new, just started in cybersecurity, and have to read these documents and figure out what the controls are and how to implement them, yes, I feel like it probably will be intimidating or challenging. (P6)

3.3.3.4 *Conflicting Requirements*

Another theme that comes up when studying the data is that of conflicting requirements (see Table 8). This theme came up sometimes having conflicting requirements, but more often, it was noted that although there are many frameworks and other legal requirements, they usually do not conflict in a way that creates a limitation in implementing the NIST SP 800-171. Some participants noted that they were able to find ways to solve requirements from multiple frameworks through the same technical solutions. The primary times when the requirements conflicted and became a limitation was when organizations had their own internal requirements that were not necessarily focused on security and were instead focused on the business goals. The participants also noted that when this was the case, it was usually a lack of understanding or a lack of desire to invest in security (see Table 8).

Table 8

Participant Responses Supporting Conflicting Requirements Theme

Theme	Examples
Conflicting requirements	So, policies are generally written with the concept in mind that they, I am not saying that they deviate from the law, but they are not written with the concept of meeting a control framework in mind. They are written with the concept of passing their SEC audits in mind, so they do not want to proclaim or say they do something. (P7) ‘We do not always have full control of our devices’ (P1). ‘Sometimes we move too fast, and they do not do all of the proper security reviews’ (P5).

3.3.3.5 *Framework Shortfalls*

Framework shortfalls showed itself as a theme through various perspectives provided by the study participants. One such example was that the participants did not feel that the NIST 800-171 was sufficient to secure their data and that they would need to use other frameworks to ensure that they were covering their bases. The data also showed that as the NIST SP 800-171 has matured and changed over time, some participants felt that it was getting better, but was just not quite there yet. Finding a way to ensure that any organization can implement the NIST SP 800-171 was noted as difficult because of how different organizations behaved differently, making a one-size-fits-all document difficult to implement. This idea has been addressed in the past by the document writers by creating requirements that have some interpretation to allow these organizations to find ways to implement them in their own way, which, as noted before, can create a situation where these requirements are unclear to others causing a limitation in implementation (see Table 9).

Table 9

Participant Responses Supporting Framework Shortfalls Theme

Theme	Examples
Framework shortfalls	So, in most organizations, at least the ones I have been in, I have worked for a global bank, a life insurance carrier, an auto insurance carrier, and now a storage hardware manufacturer. In no case have we used one framework as the guidance and overreaching policy for our internal policies because one size fits all just does not work. (P4) Draft revision three is making it better, not worse' (P5). 'Larger enterprises and how well they will be able to apply those controls and requirements throughout the organization is a concern' (P6).

3.3.3.6 *Information System Shortfalls*

While most of the themes of this study focus directly on the NIST SP 800-171 and other frameworks, one theme that came to the surface during the study was one where the participants felt there were shortfalls with their information systems. Meaning that there were configurations in place that would make it difficult or impossible to apply the requirements or that the system may not be well understood. One such example was where an organization did not have their network well enough documented and was unable to know exactly where the data they needed to protect was located, creating a situation where they were unable to secure just a section of the network to protect the data and instead had to try and secure the entire business information system, which led to various limitations such as scalability, cost concerns, or even enough employees to be able to manage it effectively. Additionally, as part of this theme, it was mentioned that other connected systems or partners could create shortfalls in the information system, creating limitations in implementing all of the NIST SP 800-171 requirements (see Table 10).

Table 10

Participant Responses Supporting Information System Shortfalls Theme

Theme	Examples
Information system shortfalls	'I do not know if it is cultural or management driven, but yes, it all comes back to … What does the company place first? Security or something else' (P5)? But I think the biggest problem that companies run into is a little thing we denote as one-offs. Someone says, hey, I have gotten a really great idea. And then the next thing you know, you have technology running in an environment somewhere. (P7) 'People do not even know what kind of data are lying where' (P8). 'Understanding your infrastructure and knowing the environment and studying the environment and trying to do your due diligence on what this organization has out in their environment and potential problems' (P2).

3.4 Contribution to Theory, the Literature, and the Practitioner Knowledge Base

This study was conducted to understand the limitations that organizations can encounter when implementing the NIST SP 800-171 requirements. Using the modified UTAUT as a framework and applying qualitative analysis, the goal was to answer the question, "What are the implementation limitations IT professionals must resolve for NIST SP 800-171 compliance?" There were various outcomes that were documented. Using this documentation, the questions of how this study contributes to theory, the literature, and the practitioner knowledge base are answered in the next few sections.

3.4.1 Theory

Using the modified UTAUT for this document extends the framework by showing how the framework can be used to look into areas where a cybersecurity framework can be viewed as technology and capture how these frameworks are being accepted and adopted. Applying the three categories from the framework, Possible Adoption Limitations, Cyber Threat Landscape, and Cybersecurity Standards, aided in determining how the themes fit into the overall answer to the project question.

3.4.2 Literature

This study contributed to the literature by finding a gap in the literature and attempting to gather information to address this gap. There has been a great deal of literature referencing other cyber security frameworks, such as NIST SP 800-53, but finding literature addressing the limitations for compliance with NIST SP 800-171 is difficult. As highlighted in the literature review, there are various items addressing that businesses are unable to implement the NIST SP 800-171 fully, but finding the limitations has been the goal of this study. Combining the knowledge that organizations are unable to fully implement the NIST SP 800-171 (Sera-Brynn, 2019) with the limitations found in this study, researchers and practitioners alike can start to find ways to overcome these limitations and, in part, create a more secure environment for everyone required to maintain CUI in their organizations.

3.4.3 Practitioner Knowledge Base

The practitioner knowledge base then can be extended through the understanding of where these limitations come from. During the study, there were many specific items that were mentioned, such as funding, lack of staff knowledge, pushback, and external factors, which, taken individually, shows a list of items that can impede implementation, but using all of the information from the literature and the study takes it one step further and highlights some themes that get to the root of why these items exist. The literature review itself had similar information for similar cybersecurity frameworks, but many of them were not applicable to businesses in the industry, and the requirement for these businesses to follow the NIST SP 800-171 was largely unaddressed.

3.5 Project Application and Recommendations

The application of this project can be through the use of the knowledge gathered during the study. Organizations are asked every day to do more with less, and finding ways to overcome limitations is a key factor in success for these organizations. Using the data gathered in this study, organizations can pinpoint the source of these limitations and address them. During the interview process, various professionals in the field answered questions relating to these limitations, and this information was used to find the most impactful or highest incidents of limitations and categorize them into themes. By addressing these themes first, organizations could then prioritize and strategize ways to overcome these limitations and then successfully implement the NIST SP 800-171 in their organization.

The primary recommendation for this study would be for a future researcher to use it to build upon and find more information that can be used to further assist these organizations in their implementation journey. One such future research topic may be to extend this study to address the newly developed Cybersecurity Maturity Model Certification and how it succeeds in the use of the NIST SP 800-171 in organizations.

3.6 Conclusion

Through the process of doing this project, various factors became known in determining what limitations organizations face when implementing the NIST SP 800-171 guidelines. The primary result that was discovered is that lack of resources is a big hurdle when it comes to the implementation of these tools. While lack of resources is a large theme, included in this theme were items such as third-party tools, fatigue, funding, finding and hiring skilled IT staff, and others. Each of these minor issues by itself can limit the adoption of certain sections of the NIST guidelines. Still, it was not until the overall analysis was performed that it highlighted the root of the problem, which is how organizations interact with the documents.

The second finding in this study was related to business culture concerns such as business priorities, internal policies and procedures, management buy-in, and resistance to change. These items were all a part of an aspects of business culture theme that, when addressed, shows things that come from within the organization and create limitations for NIST SP 800-171 implementation.

In all, the literature reviews, the continuous learning, and the study for this project all worked together to give the researcher a greater perspective on the implementation of NIST SP 800-171 guidelines while also educating on the process of gathering information and synthesizing it to create better data that can be used not only in the field as a whole, but with other learners looking to further their knowledge.

REFERENCES

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. Paper presented at the - *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA),* 1-5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Aljumaili, T. (2018). *Exploring the information security policies and practices required by small and medium-sized IT enterprises* (Publication No. 10975031). [Doctoral dissertation, Colorado Technical University]. ProQuest Dissertations and Theses Global.

Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting information security risk management challenges: A practice perspective. *Information and Computer Security, 27*(3), 358-372. https://doi.org/10.1108/ics-09-2018-0106

Bonnema, J. (2018). *5 reasons why your organization should adopt the NIST cybersecurity framework.* https://www.thesecurityawarenesscompany.com/2017/08/03/5-reasons-organization-adopt-nist-cybersecurity-framework

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

Brinkmann, S. (2012). *Qualitative inquiry in everyday life: Working with everyday life materials.* Sage Publications, Inc.

Brook, C. (2018). *What is NIST SP 800-171?* https://digitalguardian.com/blog/what-nist-sp-800-171

Brown, E. (2016). Cybersecurity 'Rosetta Stone' celebrates two years of success. *Targeted News Service* (Publication No. 1766601211). ProQuest Dissertations & Theses Global.

Chancey, T. (2022). *Why use the NIST Cybersecurity Framework?* Scarlett Cybersecurity Services. https://www.scarlettcybersecurity.com/why-use-the-nist-cybersecurity-framework#:~:text=1%20Countless%20organizations%20around%20the%20world%20use%20the,and%20every%20organization%20uses%20it%20differently%20More%20items

Cybersecurity and Infrastructure Security Agency. (2022). *Defense Industrial Base Sector*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/defense-industrial-base-sector

Cisternelli, E. (2022). *7 cybersecurity frameworks that help reduce Cyber Risk*. Bitsight Blog. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

Clapper, J., Lettre, M., & Rogers, M. S. (2017). Foreign cyber threats to the United States. *Hampton Roads International Security Quarterly, 1*.

Clarke, R., & Knake, R. (2020). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.

CMMC Accreditation Body. (n.d.). *Where do I fit in the CMMC-AB ecosystem?* CMMC. https://cmmcab.org/

Complyup. (2022). *What are the Steps Involved with Becoming NIST 800-171 Compliant? Where do I Begin?* ComplyUp. https://complyup.com/knowledge-base/

Cooper, D., Schindler, P., & Sharma, J. (2018). *Business research methods* (12th ed.). McGraw Hill Education.

Cope, D. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*, 89-91. https://doi.org/10.1188/14.ONF.89-91

Creswell, J. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage Publications, Inc.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982-1003. https://doi.org/10.1287/mnsc.35.8.982

Dedoose. (n.d.). *Home*. Dedoose. https://www.dedoose.com/

DFARS. (2020). *Defense federal acquisition regulation supplement: Assessing contractor implementation of cybersecurity requirements (DFARS case 2019-D041)*. Federal Register. https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

Dolan, K. (2022). Cybersecurity risk assessment platform for state government. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4009348

Doubleday, J. (2018). Draft guidance could spell trouble for contractors lagging on cybersecurity. *Inside the Pentagon*, *34*(18).

Edwards, S. (2017). *A detailed review of NIST SP 800-171*. Summit 7. https://info.summit7.us/blog/a-detailed-review-of-nist-sp-800-171

Elnagdy, S. A., Qiu, M., & Gai, K. (2016, June). *Understanding taxonomy of cyber risks for cybersecurity insurance of financial industry in cloud computing*. In 2016 IEEE 3rd 120

International Conference on Cyber Security and Cloud Computing (pp. 295-300). https://doi.org/10.1109/CSCloud.2016.45

FAR. (2023). *DFARS*. 252.204-7012 Safeguarding covered defense information and cyber incident reporting. *Acquisition.gov*. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

Federal Register. (2018, April 24). *The federal register*. Federal Register: Request Access. https://www.federalregister.gov/documents/2018/04/24/2018-08554/dod-guidance-for-reviewing-system-security-plans-and-the-nist-sp-800-171-security-requirements-not

Federal Register. (2020). *The federal register*. Federal Register: Request Access. https://www.federalregister.gov/documents/2020/08/31/2020-18645/defense-federal-acquisition-regulation-supplement-use-of-supplier-performance-risk-system-sprs#:~:text=The%20proposed%20rule%20amends%20the%20DFARS%20to%3A%20%281%29,SPRS%20system-generated%20item%2C%20price%2C%20and%20supplier%20risk%20assessments.

FedRAMP. (2021). *How to become FedRAMP authorized*. FedRAMP.gov. https://www.fedramp.gov

Ginn, G. M., & Munn, S. L. (2019). Interviews: Learning the craft of qualitative research interviewing, third edition, by Svend Brinkmann and Steinar Kvale. Sage Publications, Inc., 2015. 405 pages, $60.00 (paperback). *New Horizons in Adult Education and Human Resource Development*, *31*(2), 67-69. https://doi.org/10.1002/nha3.20251

Granneman, J. (2019). Fitting cybersecurity frameworks into your security strategy. *Information Security*, *20*(3), 1-1.

Harrington, D. (2022). *NIST 800-171 compliance checklist and terminology reference. Varonis.* https://www.varonis.com/blog/nist-800-171#importance-of-complying

Hawes, J. L. (2018). DoD guidance for reviewing system security plans and the NIST SP 800-171 security requirements not yet implemented. *Federal Register*, *83*(79). https://www.gpo.gov/fdsys/pkg/FR-2018-04-24/pdf/2018- 08578.pdf

Henry, P. (2015). *Why relying on network perimeter security alone is a failure.* TechTarget. https://www.techtarget.com/searchsecurity/tip/Why-relying-on-network-perimeter-security-alone-is-a-failure

Hiscox. (2022). *Hiscox cyber readiness report 2022*. Hiscox Group. https://www.hiscoxgroup.com/cyber-readiness

Imsand, E., Tucker, B., Paxton, J., & Graves, S. (2019). A survey of cyber security practices in small businesses. *Advances in Intelligent Systems and Computing*, pp. 44-50. https://doi.org/10.1007/978-3-030-31239-8_4

Jakkal, V. (2022). Cybersecurity threats are always changing—Staying on top of them is vital, getting ahead of them is paramount. *Microsoft Security Blog*. https://www.microsoft.com/en-us/security/blog/2022/02/09/cybersecurity-threats-are-always-changing-staying-on-top-of-them-is-vital-getting-ahead-of-them-is-paramount/

Jefcoat, K. R., Baxtresser, D. W., Maddoux, M. L., & Hollander, S. E. (2018). U.S. government's new focus on cybersecurity. *Pratts, Government Contracting Law Report*, *4*(7). https://www.ebglaw.com/wp-content/uploads/2018/03/Pratts-March-2018-Selby-Mitchell.pdf

John, W. S., & Johnson, P. (2004). The Pros and cons of data analysis software for qualitative research. *Journal of Nursing Scholarship*, *32*(4), 393-397. https://doi.org/10.1111/j.1547-5069.2000.00393.x

Kendall, K. L., & Long, W. E. (2018). Including cybersecurity in the contract mix. *DefenseAT&L Magazine* (Contingency Contracting Course. CON 234). https://www.dau.mil/library/defense-atl/blog/Including-Cybersecurity-in-the-Contract-Mix

Kenyon, B. (2019). *ISO 27001 controls: A guide to implementing and auditing*. IT Governance Publishing.

Kiriakou, C. M. (2012). *Acceptance factors influencing adoption of National Institute of Standards and Technology information security standards: A quantitative study* (Publication No. 3547143). [Doctoral dissertation, Capella University]. ProQuest Dissertations and Theses Global.

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Lacy, S., & Norfolk, D. (2014). *Configuration management: Expert guidance for IT service managers and practitioners*. BCS Learning & Development Limited

LeWinter, A. (2019). *Rise of the machines: Cybersecurity no longer lives in castles*. Edgewise. https://www.edgewise.net/blog/rise-of-the-machines-cybersecurity-no-longer-lives-in-castles

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage Publications, Inc.

Lynch, I. M. (2020). *Department of Defense Controlled Unclassified Information Compliance: The Impact on Small Business Contractors* (Publication No. 28000085). [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations and Theses Global.

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *AISHE-J*, *9*(3). https://ojs.aishe.org/index.php/aishe-j/article/view/335.

Marin, M. (2021). *Explaining cybersecurity threats in a decision-maker context.* GCN. https://gcn.com/cybersecurity/2017/01/explaining-cybersecurity-threats-in-a-decision-maker-context/312698/

Microsoft. (2018). Security baselines should underpin efforts to manage cybersecurity risk across sectors. *Microsoft Blog.* https://www.microsoft.com/en-us/cybersecurity/blog-hub/Security-baselines-underpin-riskmanagement.

Mutune, G. (2022). *23 top cybersecurity frameworks*. CyberExperts.com. https://cyberexperts.com/cybersecurity-frameworks/

Myauo, M. (2016). The U.S. Department of Defense cyber strategy: A call to action for partnership. *Georgetown Journal of International Affairs*, *17*(3), 21-29.

NASA, GSA, & DOD, Federal Acquisition Regulation1-1-53-1. (2022). U.S. Government Printing Office. https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf

National Archives and Records Administration. (2010). *Executive Order 13556 - Controlled unclassified information*. National Archives and Records Administration. https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

National Institute of Standards and Technology [NIST]. (2019). *NIST Updates SP 800-171 to help defend sensitive information from cyberattack*. U.S. Department of Commerce. https://www.nist.gov/news-events/news/2019/06/nist-updates-sp-800-171-help-defend-sensitive-information-cyberattack

National Institute of Standards and Technology [NIST]. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

National Institute of Standards and Technology [NIST]. (2020a). *Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary?index=A

National Institute of Standards and Technology [NIST]. (2020b). *Security and Privacy Controls for Information Systems and Organizations*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

National Institute of Standards and Technology [NIST]. (2020c). *Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/security_assurance

National Institute of Standards and Technology [NIST]. (2020d). *Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/risk_management

National Institute of Standards and Technology [NIST]. (2020e). *Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/national_institute_of_standards_and_technology

National Institute of Standards and Technology [NIST]. (2020f). *Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/penetration_testing

National Institute of Standards and Technology [NIST]. (2020g). *Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/risk_management_framework

National Institute of Standards and Technology [NIST]. (2023a). *CUI Series: Pre-Draft Call for Comments*. https://csrc.nist.gov. https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information/call-for-comments

National Institute of Standards and Technology [NIST]. (2023b). *NIST SP 800-171 Update Status*. https://csrc.nist.gov/. https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information/call-for-comments

NCU. (n.d.). *Libguides: Chapter 4: Chapter 4: Trustworthiness of qualitative data*. Trustworthiness of qualitative data - Chapter 4 - LibGuides at Northcentral University. https://resources.nu.edu/c.php?g=1007180&p=7392379

Nero, R. L. (2018). *Risks, benefits, and perceived effectiveness of outsourcing it networksecurity in small businesses: A multiple-case study* (Publication No. 10790920). [Doctoral dissertation, Capella University]. ProQuest Dissertations and Theses Global.

Nichols-Jackson, P. (2016). *Beyond compliance as a standard: A market failures approach to business ethics for small business government contractors* (Publication No. 10101047). [Doctoral dissertation, Georgetown University]. ProQuest Dissertations and Theses Global.

Noonan, E. (2022, November 10). *CMMC 2.0: POA&M requirement changes*. CyberSheath. https://cybersheath.com/cmmc-2-0-poam-requirement-changes/

Office of the Under Secretary of Defense for Acquisition & Sustainment. [OUSDAS] (2020). Defense federal acquisition regulation supplement. https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

Office of the Under Secretary of Defense for Acquisitions & Sustainment [OUSDAS]. (2023). *Cybersecurity maturity model certification (CMMC)*. https://dodcio.defense.gov/CMMC/About/

Pabrai, U. A. (2022). *What cyberprofessionals should know about CUI*. ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-8/what-cyberprofessionals-should-know-about-cui

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing, 13*(1), 103-128. 10.1108/JGOSS-05-2019-0042 https://doi.org/10.1108/JGOSS-05-2019-0042

Patterson, J. (2017). *Cyber-security policy decisions in small businesses* (Publication No. 10680962). [Doctoral dissertation, Walden University]. ProQuest Dissertations & Theses Global.

Peters, H. M. (2022). Defense Acquisitions: DoD's Cybersecurity Maturity Model Certification Framework. *Defense AR Journal, 29*(2), 178.

Purplesec. (2022). *2021 Cyber security statistics: The ultimate list of stats, data & trends.* PurpleSec. https://purplesec.us/resources/cyber-security-statistics/

Ramsay, W. (2015). *Assisting small businesses in cyber security planning and implementation* (Publication No. 1605200). [Masters Dissertation, Utica College]. ProQuest Dissertations &Theses Global.

Reed, J. (2022). *The cost of a data breach for government agencies*. Security Intelligence. https://securityintelligence.com/articles/cost-data-breach-government-agencies/

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021). *Protecting controlled unclassified information in nonfederal systems and organizations*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

RSI Security. (2021). NIST 800-171 Security baseline. *RSI Security Blog*. https://blog.rsisecurity.com/nist-800-171-security-baseline/

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-115/final

Schwartz, S. (2021). *What happens if threat data isn't shared?* Cybersecurity Dive. https://www.cybersecuritydive.com/news/information-sharing-threat-intelligence-analysis-cybersecurity/599319/

Security Magazine. (2020). *76% of cybersecurity leaders face skills shortage*. Security Magazine RSS. https://www.securitymagazine.com/articles/92312-of-cybersecurity-leaders-face-skills-shortage

Sera-Brynn. (2019). Reality check: Defense industry's implementation of NIST SP 800-171. http://web.archive.org/web/20191218042908/https://sera-brynn.com/wp-content/uploads/2019/05/Reality_Check_DFARS_2019.pdf

Sera-Brynn. (2020). Reality check: Defense industry's implementation of NIST SP 800-171. https://sera-brynn.com/wp-content/uploads/2021/08/Reality-Check-2020_web_version.pdf

Simonova, A. (2020). *An analysis of factors influencing National Institute of Standards and Technology cybersecurity framework adoption in financial services: a correlational study* (Publication No. 27998512). [Doctoral dissertation, Capella University]. ProQuest Dissertations and Theses Global.

Simplilearn. (2022). *What is a cyber security framework: Overview, types, and benefits*. Simplilearn.com. https://www.simplilearn.com/what-is-a-cyber-security-framework-article

Spencer, T. (2019). *What is the NIST SP 800-171 and who needs to follow it?* NIST. https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0

Sundararajan, V. (2022). *Assessing common control deficiencies in CMMC non-compliant DoD contractors.* [Master's Thesis, Walden University]. https://doi.org/10.25394/PGS.20200112.v1

Sundararajan, V., Ghodousi, A., & Dietz, J. E. (2022). The most common control deficiencies in CMMC non-compliant DOD Contractors. *2022 IEEE International Symposium on Technologies for Homeland Security (HST)*. https://doi.org/10.1109/hst56032.2022.10025445

Troia, V. (2018). *The cybersecurity framework as an effective information security baseline: A qualitative exploration* (Publication No. 10933040). [Doctoral dissertation, Capella University]. ProQuest Dissertations and Theses Global.

Tryon, M. (2018). Small and mighty: Cybersecurity for small and midsize businesses [web log]. https://gblogs.cisco.com/ca/2018/10/11/small-and-mighty-cybersecurity-for-small-and-midsize-businesses.

Tuttle, H. (2021). 2020 Cyberrisk landscape. *Risk Managment*, *67*(1), 21-25. https://search.proquest.com/docview/2504872398

Twin, A. (2021). *Outsourcing.* Investopedia. https://www.investopedia.com/terms/o/outsourcing.asp#:~:text=Outsourcing%20is%20the%20business%20practice%20of%20hiring%20a,usually%20undertaken%20by%20companies%20as%20a%20cost-cutting%20measure

United States. (1978). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* The Commission. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

U.S. Department of Defense Inspector General. (2018). *Logical and physical access controls at missile defense agency contractors' locations* (Report No. DODIG-2018-094). https://media.defense.gov/2018/Apr/02/2001898150/-1/-1/1/DODIG-2018-094.PDF

U.S. Government Accountability Office. (2017). *Small business research programs: Status of prior recommendations.* (No. GAO-17-594T). U.S. Government Accountability Office. https://www.gao.gov/products/gao-17-594t

U.S. Information Security Oversight Office. (2018). *2017 Report to the President.* https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342-365. https://doi.org/10.1287/isre.11.4.342.1187

Venkatesh, V., Thong, J., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, *17*(5), 328-376. https://doi.org/10.17705/1jais.00428

Vergun, D. (2022). DOD Working to Improve Cybersecurity for Its Industrial Base. Defense.Gov https://www.defense.gov/News/News-Stories/Article/Article/2953204/dod-working-to-improve-cybersecurity-for-its-industrial-base/#:~:text=The%20Defense%20Department%27s%20industrial%20base%20is%20huge%2C%20encompassing,for%20the%20department%2C%20the%20companies%20and%20national%20security.

Verizon. (2022). *2022 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Violino, B. (2022). *Rising premiums, more restricted cyber insurance coverage poses big risk for companies*. CNBC. https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-

.html#:~:text=Cyber%20insurance%20premiums%20increased%20by,companies%20to%20afford%20or%20obtain.

Vistage. (2018). Cyberthreats and solutions for small and midsize businesses: A framework for mitigating risk and defending your company against a cyberattack. https://www.vistage.com/demand/cyberthreat-solutions-pdf-form/

Xie, K. (2020). *4 key challenges for cybersecurity leaders*. World Economic Forum. https://www.weforum.org/agenda/2020/01/four-key-challenges-for-cybersecurity-leaders/

Yvon, T. (2020). *Exploring factors limiting implementation of the National Institute of Standards and Technology cybersecurity framework* (Publication No. 28028658). [Doctoral dissertation, Colorado Technical University]. ProQuest Dissertations and Theses Global.