EXAMINING THE RELATIONSHIP BETWEEN FORMAL RMF TRAINING AND PERCEPTIONS OF RMF EFFECTIVENESS, SUSTAINABILITY, AND COMMITMENT IN RMF PRACTITIONERS

By

P. Devon Schall

A dissertation summary submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Ph.D.)

UNIVERSITY OF THE CUMBERLANDS

December 2018

DEDICATION

I would like to dedicate this research to my mother, Sheila Schall and my late father, Gerald Schall as well as my wife, Sarah Hill. My mother and father worked tirelessly to provide me with a rich education which I believe is the primary motivator for my drive and professional successes. My mother has also been one of my biggest supporters, and I feel I owe my intellect and writing ability to her. I am very grateful to have had parents that attended all of my childhood events and gave me immeasurable support. Thanks, Mom!

I appreciate all the sacrifices required of my wife, Sarah, and her patience as I have worked towards this goal over the length of our marriage. I recognize my career stressors have been challenging, and I don't think I could have done this without your support and patience. I look forward to spending more time with you and providing you support as we start planning to begin our family.

ACKNOWLEDGMENTS

I would like to thank my Dissertation Director, Dr. Oludotun Oni for his assistance and clear feedback throughout this process giving me the direction necessary to navigate this research. I also appreciate the efforts of my committee members, Dr. Bobbi Jo Taylor and Dr. Charles Lively. I would like to acknowledge Dr. Donnie Grimes for providing me with the knowledge of this program when it is was in early approval stages.

Additional thanks go to my friend and mentor, Dr. Samuel Jennings for his continued support in my academic and professional aspirations. In my undergraduate career, Dr. Jennings provided me with the confidence and support I needed to pursue this credential. Thank you to Dr. Katey Wilson for fielding my statistics questions and occasional research challenges. I would also like to thank my wonderful colleagues, Lon J. Berman and Kathryn Daily for giving me direction regarding navigating RMF and becoming a cybersecurity professional. Lastly, I would like to thank my extended family and Ms. Brittany Shaffer and Mr. Daniel McConnell for providing me with honest support and feedback in a personal and professional capacity.

I am blessed to have such supportive and wonderful friends and family members who have made this journey possible!

ABSTRACT

The United States Federal Information Systems Modernization Act (FISMA) included a mandate for the National Institute of Standards and Technology (NIST) to modernize and create new methods of strengthening the U.S. Government's Cybersecurity posture. NIST answered this call with the creation of Risk Management Framework (RMF). RMF has received criticism and has been viewed as ineffective and a potential failure. This quantitative research investigated the relationship between receiving formal RMF training and perceptions of RMF effectiveness, RMF commitment, and RMF sustainability. The research proposed that the receipt of formalized RMF training would increase the perceptions of RMF effectiveness, RMF commitment, and RMF sustainability in RMF practitioners. A convenience sample of 81 RMF practitioners responded to an online survey assessing perceived competence of RMF effectiveness, RMF commitment, and RMF sustainability as well as the amount of formal RMF training hours they had received. The data were analyzed utilizing statistical methods of descriptive statistics, analysis of variance (ANOVA) and Pearson's Correlations. Based on the results of this study, a significant, positive relationship exists between the receipt of formalized RMF training and perceptions of RMF effectiveness. Statistical significance can be seen in ANOVA tests where there was a significant difference in the mean effective Perceived Competency Scales (PCS) Scores among those with varied levels of formal RMF training ($MS = 5.388$), (F [2,78] = 3.645, $p < .05$). Pearson's Correlation also indicated that there was a significant positive association with the Effective PCS Score and the Amount of Training Received Category, ($r = .253$, $n = 81$, $p = .023$). Understanding the relationship between perceptions of RMF effectiveness and

the receipt of formalized RMF training may be helpful in driving effective RMF implementation throughout the U.S. Government and contractor community minimizing the likelihood that U.S. Government systems are compromised via cybersecurity breaches.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

Introduction

Cybersecurity attacks dominate the news as their likelihood of occurrence has grown exponentially in the past decade. No enterprise or individual is immune in being vulnerable to the threat of a cybersecurity attack. New corporate executive roles have been established such as Chief Information Systems Security Officer (CISSO), and the education training sector is responding with an uptick in cybersecurity course offerings (NICCS, 2017). The speed of technology growth, as well as the Internet of Things (IoT), can be attributed to the upsurge in cybersecurity breaches impacting government agencies as attack surface areas are increasing (Bryce, 2017).

In 2017, the number of cybersecurity attacks nearly doubled from 82,000 in 2016 to 159,700 in 2017 (Cyber Incident & Breach Trends Report, 2018). Organizations such as the Federal Deposit Insurance Corporation (FDIC) and the Internal Revenue Service (IRS) reported serious cybersecurity attacks (Walter, 2018). Government agencies such as the Department of Defense (DoD) were not spared in the influx of these incidents (Walter, 2018).

A variety of cybersecurity frameworks exist with their general overall objective being that of hardening technology infrastructure to defend against cybersecurity attacks. These cybersecurity frameworks are focused on a variety of industries and unique organizational structures have their own defined frameworks (Hussain, 2017). In the U.S., the Federal Information Systems Management Act of 2002 (FISMA), later updated

in 2014 to the Federal Information Systems Modernization Act included a mandate for the National Institute of Standards and Technology (NIST) to modernize and create new methods of strengthening the U.S. Government's cybersecurity posture (Federal Information Systems Management Act of 2002, 2002). NIST answered this call with the creation of the Risk Management Framework (RMF) (Joint Task Force Transformation Initiative, 2004). RMF is mandated by the U.S. Government as their prescribed cybersecurity framework. RMF has come under increased scrutiny as not being successfully implemented which puts the confidentiality, integrity, and availability of the U.S. Government's data and assets at risk (Maclean, 2017). It has been proposed that the availability of more formal training offerings could mitigate the poor implementation of RMF (Webb, 2015).

Statement of the Problem

Over the past decade, the U.S. Government has experienced a variety of cybersecurity breaches and information technology process errors that could have been mitigated through proper implementation of RMF. A prime example of this can be seen in the 2015 US Office of Personnel Management (OPM) cybersecurity breach in which personnel records of 21.5 million government staff and contractors were leaked (Cyber Incident & Breach Trends Report, 2018). Other examples include a Tricare breach in 2011 where several million users of government health services had their personal health information (PHI) compromised due to government contractor errors (Leonard, 2015). The National Archives and Records Administration (NARA) in 2018 also had 76 million records of veterans exposed due to a hard drive being sent out for repair and not properly

sanitized (Leonard, 2015). All issues above could have potentially been avoided through proper implementation of RMF.

Another concern with RMF is the excessive amount of required documentation which cannot keep pace with the agility and speed of hackers exploiting vulnerabilities (Maclean, 2017). In contrast, the U.S. Government's cybersecurity teams often reveal security vulnerabilities through penetration testing and then requirements such as the meeting of change control boards (CCB) and approval changes can create weeks to months for vulnerabilities to be mitigated and cost as much as $25,000 for something as simple as a basic password policy documentation change to be implemented (Maclean, 2017). Again, through proper RMF training, these documentation and agility issues could be addressed and baseline corrective actions could be put into place. An example of a corrective action would be a policy for critical threats triggering an immediate meeting of the CCB as well as training on not overestimating costs in the Plan of Milestones and Actions (POA&M).

Other major problems relating to RMF efficiency have been stated as an assumption of unlimited time and financial resources due to the thousands of required security assessment procedures as well as security control documentation bloat (Jackson, 2017). The immense amount of resources required for RMF also often distracts from mission goals and overall security postures (Jackson, 2017). In essence, NIST has created a highly complicated cybersecurity policy that does not translate well in application leaving security gaps (Jackson, 2017). Through proper training, many of these RMF shortfalls can be addressed and mitigated. A correct process of applying RMF exists, but most practitioners do not have the education to implement it correctly (Jackson, 2017).

Unfortunately, RMF reports submitted to OMB are indicating that RMF is not producing satisfactory results which creates a need for increased policy commitment and RMF efficiency analysis (Jackson, 2017).

It is a serious and immediate concern of the DoD community that U.S. Government systems are not properly hardened to prevent cybersecurity breaches (Jackson, 2017). If DoD systems are left vulnerable, the U.S. Government exposes itself to cybersecurity attacks which could lead to catastrophic losses of life. Due to the lack of appropriate RMF training resources, the RMF process is not being applied properly which is greatly increasing the risk for these grave consequences (Blake, 2018). Government agencies do not have appropriate budgets to allow for delivery of RMF training (Jackson, 2017). Budget constraints often top the list of RMF obstacles with untrained internal threats a close second (Daily, 2017). Due to these RMF budgeting shortages, RMF duties are often assigned to entry-level government or government contractor personnel who have little to no cybersecurity or RMF experience (Assi, 2018). These unskilled RMF workers have subpar implementation abilities which lead to RMF projects getting out of scope from a time, financial, and overall cybersecurity protection standpoint.

Purpose of Study

The purpose of this investigation and survey research is to determine how formal RMF training received by an RMF practitioner influences their perceived confidence in RMF effectiveness, RMF compliance commitment, and the long-term sustainability of RMF as a cybersecurity framework for the U.S. Government. This study can provide a

better understanding of the need for additional training resources for RMF in the U.S. government and private industry. This research is intended to be used as a resource for leadership and administrators in government agencies as well as the contractor community to aid and guide in the training policy development process for RMF education with the end goal of creating a coherent understanding of RMF and proper RMF implementation.

Hypothesis Statement

The following hypothesis statement revolves around the related problems of perceived RMF effectiveness, RMF commitment, and RMF long-term sustainability that motivated this study.

It is hypothesized that perceived RMF confidence ratings relating to effectiveness, compliance commitment, and long-term sustainability of RMF as the U.S. Government's cybersecurity framework will increase in RMF practitioners who have received formalized RMF training. This increase in perception will be due to formalized training providing RMF practitioners a comprehensive understanding of the proper application of RMF. The data collected in this study will demonstrate a need for formalized RMF training, making the exhaustive policy efforts of the U.S. Government in the creation of RMF more successful due to RMF practitioners gaining the ability to fully comprehend RMF goals and objectives.

Previous Studies

The topic of RMF has not been studied extensively at an academic level. Most of the available literature on RMF consists of white papers, newsletters, and conference presentations. Specifically, no studies have been conducted on RMF and the relationship it has with formal training methodologies. RMF practitioners and executives are frustrated and have indicted RMF is failing in meeting the goals and objectives it defines for itself, but minimal research has been conducted on viable solutions to combat these perceived failures. This study seeks to bring value and advance the analysis of the ways in which RMF can be successful with a goal of curbing the recent trend of blaming NIST in creating cumbersome ineffective cybersecurity policy.

Limitations of the Study

Despite the researcher's best efforts, the results of this study may be affected by the following limitations:

1. This study utilized an online survey instrument; therefore, the condition of survey completeness and accuracy by individual participants is uncertain.
2. Students may not have felt they were able to be completely honest due to their employment relationships as U.S. Government personnel implementing a U.S. Government mandated framework. This bias was combated with anonymous surveys.

Assumptions

The study was conducted with assumptions that the RMF practitioners utilized in the survey would volunteer because of their personal interest in the topic under study,

possess a baseline understanding of RMF, and provide honest responses. This baseline understanding of RMF allowed participants the ability to understand the context of the questions and research goals.

Definitions of Terms

The following definitions were used in the study:

Authorizing Official (AO): Senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (Nieles, Dempsey, & Pillitteri, 2017).

Availability: The property of being accessible and useable upon demand by an authorized entity (Kissel, 2013).

Chief Information Systems Security Officer (CISO): Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers (Kissel, 2013).

Confidentiality: The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information (Kissel, 2013). Confidentiality is often achieved through cryptographic means which are outlined in FIPS 199 (National Institute of Standards and Technology, 2004).

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks (Kissel, 2013).

Cybersecurity Active Attack: An attack that alters a system or data (Kissel, 2013).

Federal Information Systems Modernization Act (FISMA): A statute that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB (Kissel, 2013).

Integrity: The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner (Kissel, 2013).

Intrusion: An unauthorized act of bypassing the security mechanisms of a system (Kissel, 2013).

Risk Management Framework (RMF): A six-step process that emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems (Joint Task Force Transformation Initiative, 2018).

Security Controls Assessment: The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and

producing the desired outcome with respect to meeting the security requirements for the system (Kissel, 2013).

Security Controls Assessor: The individual, group, or organization responsible for conducting a security control assessment (Kissel, 2013).

Security Control Baseline: The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection (Kissel, 2013).

Summary

This chapter presented an overview and purposes of the research. RMF practitioners cannot keep pace with the agility and speed of hackers exploiting vulnerabilities (Maclean, 2017). This lack of efficiency is due to a global misunderstanding of RMF which is occurring due to a lack of formal RMF training. RMF is a complicated process which requires formalized training for effective application. Through appropriate budgeting and an increased focus on RMF training, the RMF process can be more substantially improved and made more effective. Formalized training will also increase RMF practitioner commitment and perception of long-term RMF sustainability due to the knowledge transfer which is necessary for a thorough understanding of the highly complicated process. RMF has been documented as being a strong cybersecurity policy on paper, but the application of this policy is creating immense confusion and frustration which can be remediated through formalized RMF education (Kohnke, Sigler, & Shoemaker, 2016). The next chapter provides a review of literature comprised of U.S. Government RMF policy guidance documentation, literature

on RMF effectiveness, a survey of formal IT training effectiveness research, and learning theory application to compliance training data.

CHAPTER TWO

REVIEW OF THE LITERATURE

Introduction

The following literature review will present the current range of artifacts that relate to major RMF related U.S. government policies, U.S. government guidance on cybersecurity, RMF implementation guidance, IT training research, and an analysis of learning theories that are best suited for compliance training. The research strategy in identifying artifacts included a Google Scholar, ProQuest, as well as an extensive search through the National Institute of Standards and Technology (NIST) databases on keywords established through collaboration with RMF subject matters experts. Key search words included: Risk Management Framework, RMF, Cybersecurity Framework, CSF, Learning Theories, FISMA, National Institute of Standards, NIST, Risk Management Framework Effectiveness, RMF Effectiveness, Risk Management Framework Commitment, RMF Commitment, Risk Management Framework Sustainability, RMF Sustainability, Risk Management Framework Training, RMF Training, Cybersecurity Training, and IT Training. Due to the highly focused niche dynamics of the topic being researched, older literature (written before 2013) was included in this literature review. Older literature was evaluated on a case by case basis for relevance to the proposed study.

Early Cybersecurity Guidance

A new era of cybersecurity dawned with the 1983 publication of *Guidelines for Computer Security Certification and Accreditation* (FIPS 102), which was one of the earliest cybersecurity guidance documents published by the National Bureau of Standards (NBS) later renamed the National Institute of Standards and Technology (NIST). FIPS 102 is one of the first government artifacts that refers to Assessment and Authorization (A&A) in the realm of cybersecurity. At the highest level, A&A is the U.S. Government's attempt at creating an approval chain for information technology systems connecting to a network (Guidelines for Computer Security Certification and Accreditation, 1983). An example of A&A would be the requirements for a mobile device to connect to a U.S. government network. For a mobile device to connect to a U.S. government network, the mobile device would need to go through a cybersecurity compliance process with the end goal of achieving a formal connection approval (Department of Defense, 2014). FIPS 102 is often seen as the birthplace of A&A in the U.S. Government. In comparison to current NIST guidance documents, FIPS 102 presented very early definitions and requirements for the connection of information technology systems. In the coming decades, hundreds of documents on cybersecurity guidance and A&A would be published by NIST. These documents resulted in the most current iteration of A&A guidance titled, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and the accompanying document *Risk Management Framework (RMF) for DoD Information Technology (IT)* which goes into greater depth in describing RMF for DoD IT.

Risk Management Framework (RMF)

In the U.S., the Federal Information Systems Management Act of 2002 (FISMA), later updated in 2014 as the Federal Information Systems Modernization Act included a mandate for NIST to modernize and create new methods of strengthening The U.S. Government's cybersecurity posture. NIST answered this request with RMF. RMF is a structured process that integrates information security and risk management activities into the system development life cycle. (Joint Task Force Transformation Initiative, 2014). The RMF Life Cycle consists of a six-step process with each step outlined in Figure 1.

Source NISP SP 800-37 R1

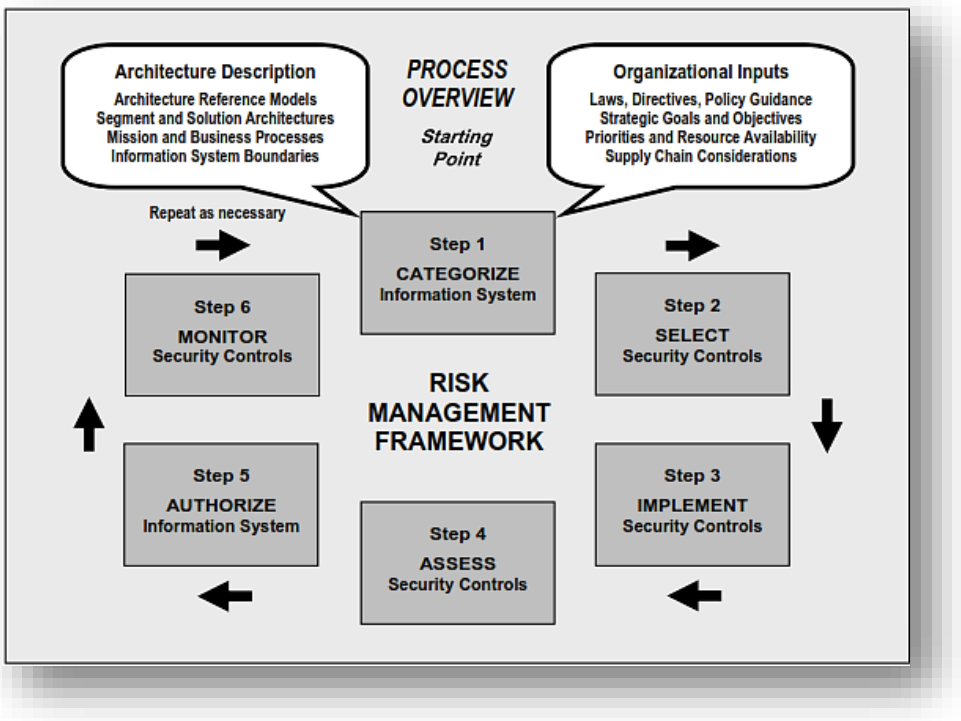

Figure 1. RMF Life Cycle six-step process.

As shown in Figure 1, the RMF process culminates with Step 5 requiring an Authorizing Official (AO) granting three possible approval outcomes.

1. Authorization to Operate (ATO)
2. Denial of Authorization to Operate (DATO)
3. Interim Authorization to Test (IATT)

The decisions above are based on an evaluation of the overall cybersecurity risk of a system in relation to implemented security controls (Joint Task Force Transformation Initiative, 2014). It is well known in the government compliance community that RMF is a very complicated framework with many variables. The most important baseline aspects of RMF to understand in relation to this research are:

1. RMF is required for any system to connect to a network in the U.S. Government.
2. RMF is a time intensive and highly complicated process involving collaboration between many stakeholders.
3. Systems are initially evaluated for their levels of confidentiality, integrity, and availability (CIA) which are then rated on a scale of low, moderate, or high based on the types of information the system processes. Once the types of information a system processes are established, NIST 800-60 volumes I and II provide a baseline system categorization (Stine, Kissel, Barker, Lee, & Fahlsing, 2008). The system categorization established from the CIA baseline dictates how many security controls are assigned to the system (Bond, 2004). That number of security controls can easily be hundreds with more granular assessment procedures in the thousands. Each one of these controls and assessment procedures must be responded to via implementation statements and the inclusion of possible documentation artifacts.

4. The final decision for an ATO comes from an AO who is generally a high-ranking government employee who may or may not have a background in information technology. With AO's operating at an executive level, concerns have been expressed in the AO's understanding of RMF fundamentals as well as the underlying technology associated with the specific systems they are authorizing (Blake, 2018).
5. ATO's are granted with a maximum timeframe of three years. At the conclusion of the three-year interval, systems must begin the RMF process again which is time and resource heavy often taking a minimum of nine months to complete (Metheny, 2013).
6. An important aspect of RMF is the concept of Information System Continuous Monitoring (ISCM). Through ISCM, systems achieve an ATO and they are continuously monitored for changes in system status that may potentially influence their cybersecurity posture (Dempsey, Chawla, Johnson, Johnston, Jones, Orebaugh, 2011). The authors of RMF have a goal of ISCM eliminating the idea that RMF is a compliance "check the box" process geared at reaching an ATO and then being forgotten about for three years until renewal.

Checkbox Compliance & Lack of Incentives

Due to RMF being a government requirement, many people completing RMF see it as a "check the box" process with the goal of achieving an ATO in the most efficient means possible (MacLean, 2017). This "check the box" mentality is very dangerous to the nation's cybersecurity posture and not in the spirit intended by NIST in the creation

of RMF (Blake, 2018). In a survey based on RMF compliance by SolarWinds, over 70% of respondents comprised of Federal, civilian government agencies, and DoD agreed that being compliant with "check the box" processes do not necessarily equate to secure cybersecurity postures (SolarWinds Federal Cybersecurity, 2017).

Many organizations do not see the need for proper cybersecurity preventive measures until it is too late (Blake, 2018). The converse of this mentality would be long-term strategic planning for the hardening of cybersecurity infrastructure. Another primary trend encouraging this "check the box" compliance is a lack of incentive for civil servants to complete their projects with elevated levels of performance (Maclean, 2017). Unfortunately, the U.S. Government does not offer incentives for going above and beyond baseline requirements in government work. For some projects such as RMF, baseline performance is not sufficient. RMF has the overall goal of protecting human life and those implementing RMF must show competence and a thorough understanding of the process. Without proper training, it is difficult for this thorough understanding to be accomplished.

Limited Agility with Poor Training

Mentioned often in RMF performance analysis, RMF can be perceived as lacking agility. As stated in *The NIST Risk Management Framework: Problems and recommendations*, the hackers that are trying to attack the national technology infrastructure are looking to expose vulnerabilities as quickly as possible. If RMF is implemented poorly by unskilled staff, extreme delays can occur in mitigating discovered vulnerabilities. For changes to occur in RMF, they must be reviewed by a committee

called a Change Control Board (CCB). Untrained RMF practitioners may configure these groups to only meet monthly. This lack of agility results in delays in reconfiguring systems which often leads to vulnerabilities being exploited. Through proper training of the correct implementation of RMF, these delays can be minimized (Smith, 2018).

Cybersecurity Framework (CSF)

The U.S. President, Donald J. Trump issued Executive Order 13636,7 entitled "Improving Infrastructure Cybersecurity" which tasked NIST with creating a voluntary cybersecurity framework for critical infrastructure (Tran, 2015). NIST then proceeded to publish another set of documentation which mandates cybersecurity requirements titled Cybersecurity Framework (CSF) consisting of a five-step process isolated from RMF's six-step process (National Institute of Standards and Technology, 2014). Unlike RMF, CSF is not required, and it does not have the function of a formal ATO as it is targeted to private industry as a voluntary framework (Shen, 2014). It is also worth noting that many experts in government policy have high hopes for CSF to become a global cybersecurity framework (Shackleford, Proia, Martell, & Craig, 2014). Even if CSF is not the current international standard, many nations are also creating their own framework modeled on CSF (Shackelford, 2016). It has been observed that CSF has much more agility and flexibility than RMF (Gyenes, 2014). To that end, in the most recent version of NIST 800-53 Rev 2, much discussion is had regarding the blending and use of CSF and RMF. CSF's future is unclear, but on May, 11, 2017 a U.S. Executive Order (EO) was issued stating that agency heads should provide a report to the Office of Management and Budget (OMB) within 90 days stating their risk status as it relates to CSF or a subsequent

framework (Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 2017). Although RMF is not directly stated in the EO referenced above, RMF is indeed a subsequent framework. Still, most critics of CSF suggest that CSF will not be implemented by the public due to it being voluntary and not required like RMF (Chung, 2018). Preliminary research has also been conducted on CSF as it relates to RMF, but the data is stark with minimal conclusions (Almuhammadi & Alsaleh, 2017).

A Case for Custom Training

"Coping with Rapid Changes in IT" written by John Benamati and Albert Lederer suggest that IT is changing at an unimaginable pace and these rapid changes in IT are creating ever-shrinking budgets with increased training demand (Benamati & Lederer, 2001). The primary focus of their article is to outline ways in which IT professionals are staying current in their daily technology landscape. Benamati and Lederer studied IT professional's 'perceived to be most effective' as well as 'actual most effective' coping mechanisms to be most successful in their growing field. A variety of questions were posed to IT workers regarding their individual perceptions and that data was later compared to the workforce implementation of coping strategies. The results of this study proved that IT professional's 'perceived most beneficial' coping strategies were often not the most effective ones (Benamati & Lederer, 2001). One of the lowest ranked coping strategies was educating IT professionals through traditional college classes which ranked 26 out of 34 (Benamati & Lederer, 2001). The highest-ranking effective methods that related directly to training were providing customized education on new IT topics

(Benamati & Lederer, 2001). With RMF considered a relatively new topic, customized RMF training would be highly effective in workforce education. The concept of custom training reflects an industry need for education to be agile and provide a strong reflection of current industry best practices.

Learning Theories for Compliance Training

Discussions of learning theories are valuable when addressing formalized custom RMF training development. The process of learning theories can be described as a permanent change in behavior and the three most popular learning theories are cognitivism, behaviorism, and constructivism (McHaney, 2011). Out of the three theories referenced, constructivism has shown great promise in teaching students complicated compliance processes such as RMF.

Constructivism is based upon the unique learning styles and experiences of individuals often integrating hands-on activities (Duffy & McDonald, 2015). In working through the multi-step processes of RMF, collaborative learning strategies such as group projects and discussions are highly effective (Duffy & McDonald, 2015). In contrast to constructivist learning theory, the U.S. Government publishes hundreds of pages of complicated RMF policy guidance which is very difficult to digest for someone not trained in the analysis of highly technical documentation. By providing proven formalized educational delivery methods utilizing constructivist learning theories students can effectively learn how to implement RMF.

Industry based training data has also shown that constructivist learning theories are highly effective in compliance training. Examples of these learning styles can be seen

in blended learning which utilizes a variety of learning styles to engage the learner (Ford, 2018). Occupational Safety and Health Administration (OSHA) believes that effective compliance training programs allow employees to participate in the learning process enabling them to create new knowledge (Ford, 2018). The training suggested by OSHA can be achieved through hands-on experiences as well as group learning and role-playing activities (Ford, 2018). Topics that lend themselves to blended learning are those that require more than a baseline knowledge of a topic like RMF. By creating real-world examples of compliance and specific RMF activities learners are more likely to be able to perform the newly learned activities in their own workplace (Ford, 2018). By mirroring real life RMF activities, a learner is more likely to be able to perform an activity in their work environment making the case for formalized RMF training which integrates blended and constructivist learning theories.

Summary

Minimal research has been conducted on RMF. At the time of this dissertation's publication, very limited peer-reviewed research has been conducted on RMF in general as well as the way in which RMF effectiveness relates to RMF practitioners having access to training. RMF has been discussed in industry articles as well as newsletter publications, but data collection has been sparse, and most of the published information is subjective. The gap in RMF research and literature is large and this dissertation looks to bridge this delta and provide concrete recommendations for the US Government in improving the effectiveness of cybersecurity efforts through formal RMF training efforts.

CHAPTER THREE

METHODS AND PROCEDURES

Introduction

This chapter describes the methodology used in investigating the associations between formal Risk Management Framework (RMF) training and perceived RMF effectiveness, RMF sustainability, and RMF commitment. This chapter will include problem restatement, statement of hypotheses, description of research design, the operational definition of variables, description of materials, description of procedures, description of instruments, description of methods in participant selection, and a description of planned data analysis techniques.

Restatement of the Problem

The U.S. Government has experienced a variety of cybersecurity breaches and I.T. process errors that could have been mitigated through proper implementation of RMF. RMF is an intricate process that requires formal training for successful implementation. Often, government agencies do not allocate enough funds to provide baseline RMF training. This funding shortage leaves those implementing RMF without adequate RMF policy knowledge which creates confusion and RMF projects quickly get out scope from a time and financial construct. Due to inadequate training, RMF is not being implemented properly which is creating extreme vulnerabilities in the U.S. Government's cybersecurity posture.

Statement of Hypotheses

Hypothesis 1 – Cognitive Load Theory

Cognitive Load Theory is a learning theory developed by John Sweller and relates to the amount of information working memory can hold at one time (Heick, 2017). Cognitive Load Theory suggests that working memory can be expanded by breaking information into smaller pieces through a technique called Chunking (Nesvig, 2014). Chunking is a strategy used to break down substantial amounts of data into smaller pieces of information, which reduces cognitive load as learner's process information (Nesvig, 2014). Often, RMF practitioners without formal training lack a thorough understanding of RMF due to the cognitive overload that exists in attempting to digest hundreds of pages of policy documentation. Through the implementation of formal RMF training backed by sound instructional design methodologies, RMF practitioners can gain a working understanding of RMF leading to an increased perception of effectiveness.

1. RMF practitioners who have received formal RMF training will perceive RMF as being effective in protecting the U.S. Government's technology infrastructure.

   H_0: There is no relationship between receiving RMF training and a positive perception of RMF effectiveness.

   H_1: There is a relationship between receiving formal RMF training and a positive perception of effectiveness.

Hypothesis 2 – Social Exchange Theory

It has been shown that employees have higher amounts of organizational commitment when they receive comprehensive training (Ehrhardt, Miller, Freeman, & Hom, 2011).

This theory is rooted in the Social Exchange Theory which theorizes a relationship has a cost and rewards basis. Through Social Exchange Theory, the act of an employer offering formal RMF training rewards an employee in the employee gaining the ability to understand a complicated concept such as RMF. The RMF practitioner then has a vested interest in committing to RMF from a compliance standpoint due to the time and financial commitment their organization has invested in them.

2. RMF practitioners who have received formal RMF training will display high levels of RMF compliance commitment.

   H_0: There is no relationship between receiving formal RMF training and a positive perception of RMF commitment.

   H_1: There is a relationship between receiving formal RMF training and a positive perception of RMF commitment.

Hypothesis 3 – Bloom's Taxonomy Model

As shown in Figure 2, Bloom's Taxonomy Model consists of six levels of knowledge types which are presented visually in the shape of a pyramid (Nevid, 2012). The higher the student rises to the top of the knowledge type pyramid the more mastery the student possesses of the subject being studied. The pyramid starts from the bottom and works to the top with labels of Remembering, Understanding, Applying, Analyzing, Evaluating, and Creating (Nevid, 2012). The very top level titled Creating demonstrates mastery of a specific topic (Nevid, 2012).

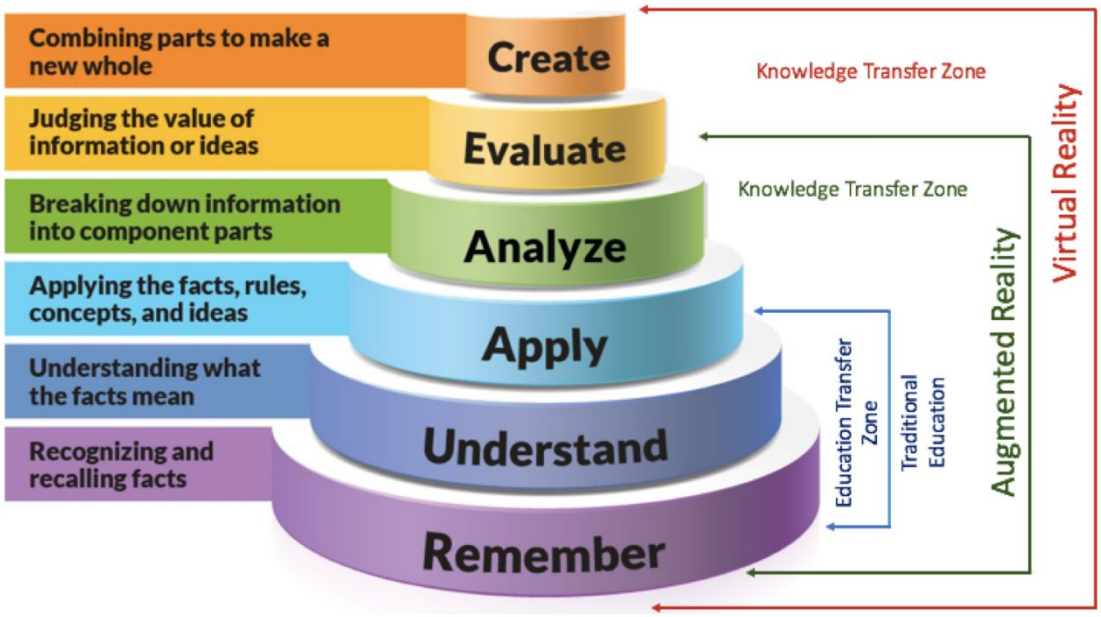

Figure 2. Blooms Taxonomy.

Since RMF is a highly complicated government policy mandated with hundreds of pages of compliance documentation, RMF practitioners without formal training do not often acquire a true understanding of the RMF process. This lack of RMF comprehension detracts from RMF practitioner's confidence in RMF being a sustainable long-term cybersecurity framework. In receiving formal RMF training, a learner has the potential to move through all levels of Bloom's Taxonomy gaining a complete understanding of RMF. This understanding will enable practitioners to analyze and evaluate the complicated elements of RMF which will increase their attitude that RMF is a sustainable long-term solution for the U.S. Government.

3. RMF practitioners who have received formal RMF training will have confidence that RMF will be a sustainable long-term cybersecurity framework for the U.S. Government.

H_0: There is no relationship between receiving formal RMF training and a positive perception of RMF long-term sustainability.

H_1: There is a relationship between receiving formal RMF training and a positive perception of RMF long-term sustainability.

Description of Research Design

Quantitative data on the perceived confidence, compliance commitment, and sustainability ratings for RMF were collected and used in this research. Survey research was implemented, and data was collected through a questionnaire. The intended participants in the study were those who work in the U.S. Government or serve as U.S. Government contractors with requirements of cybersecurity compliance in their job roles.

The survey questionnaire was provided to the members of the LinkedIn group titled Risk Management Framework (RMF) Resource Center via a survey link posted in the group as well as a private message sent to each member of the group with an explanatory invitation. This group consists of 1779 members and was established to provide its members with the opportunity to connect in understanding RMF. The survey was presented to all group members without any prior research or bias regarding their previous RMF training received or years of experience.

Operational Definition of Variables

Risk Management Framework (RMF) training

RMF is an incredibly complicated multi-step process which encompasses hundreds of pages of U.S. Government policy guidance. Often policy guidance created

by the U.S. Government can be difficult to understand and one often cannot simply read hundreds of pages of policy to utilize effective implementation. Risk Management Framework (RMF) training is instruction delivered to students in a formal instructor-led classroom-based environment teaching the intricacies and steps of RMF.

Risk Management Framework's (RMF) Effectiveness

The stated goals of RMF are to improve information security and strengthen the risk management process within the U.S. Government. Perceived effectiveness of RMF is based off an RMF practitioner's understanding of RMF strengthening the U.S. Government information security and risk management process.

Risk Management Framework Commitment

RMF is a time-intensive process which can take months or years to implement. It is difficult for an RMF practitioner to be committed to a subject that they do not fully understand. RMF compliance commitment is the long-term dedication to RMF which would include documentation maintenance and maintaining an ongoing cybersecurity posture.

Risk Management Framework's Sustainability

A variety of information security frameworks exist, and the policy makers at NIST are introducing new cybersecurity guidance regularly. A variety of other cybersecurity also framework existed before RMF. To maximize government efficiency,

it would be optimal for RMF to have long-term sustainability as the cybersecurity framework that U.S. Government implements.

Description of Procedures, Materials, & Instruments

A survey questionnaire (See Appendix D) was distributed for this study utilizing Survey Monkey. The survey questionnaire was provided to the members of the LinkedIn group titled Risk Management Framework (RMF) Resource Center. The survey was sent via a posted link as well as a private message sent to each member of the group. The perceptions of RMF practitioners being collected in this research were RMF effectiveness, RMF commitment, and RMF sustainability. The drivers of RMF practitioner's perceptions are the amount of formal RMF training received.

The Perceived Competence Scales (PCS) were used to assess the degree to which participants felt confident about the dependent variables which are RMF effectiveness, RMF commitment, and long-term sustainability of RMF in relation to the independent variable, which is training received (Deci, 2006). PCS has been used in several applications including a study of diabetic patients in which perceived competence was predicted by the degree that patients experienced autonomy in their Diabetes Treatment Centers and how the perceived competence at carrying out the treatment regimen predicted patient's glucose control (Williams, Freedman, & Deci, 1998). For this study, a survey questionnaire was distributed utilizing PCS on a scale of 1-7 assessing the degree to which participants felt confident in RMF effectiveness, RMF commitment, and RMF sustainability in relation to receiving formal RMF training. A low score on the 1-7 scale indicated minimal competence and a high score correlated to maximal competence. The

questionnaire utilizing PCS can be seen in Appendix D. The alpha reliability for the perceived competence items has always been about 0.90 (Deci, 2006)

Due to the hypotheses being structured on relationships with variables, the sample size was established based on a power of .80 for Pearson correlation coefficient (r) for large effects. The sample size needed to achieve .80 power value at .01 significance level is 41 (Cohen, 1992). Additional testing was conducted in the conclusion utilizing Cronbach Alpha to confirm validity and reliability of the research instrument.

Selection of Participants

The LinkedIn group titled Risk Management Framework (RMF) Resource Center consists of 779 RMF practitioners of varied RMF experience and RMF training backgrounds. The group is open to any individuals with an interest in RMF and learning as well as collaborating in effective implementation of RMF. The open nature of the group provided a level of randomness and sample diversity.

Ethical Consideration

Ethics are a critical element in all research studies. Research subjects were provided informed consent for the survey relating to their willingness to engage in answering survey questions. The informed consent form can be seen as referenced in Appendix B. No personal identifiable (PHI) or personal health information (PHI) was collected in research. Every effort was taken to meet ethical baselines in maintaining research integrity and validity. IRB approval was also received for this study from University of the Cumberlands (See Appendix G).

Data Analysis

A goal of quantitative research is to use statistical procedures to determine strength between variables (Cresswell, 2013). SurveyMonkey was used to collect the data from the survey and provides the ability for export in Microsoft Excel. IBM SPSS 25 statistical software package was used for descriptive and inferential statistical analysis. Statistical methods, such as an analysis of variance (ANOVA) and correlations tests were used to analyze data and test the hypotheses. Descriptive statistics including means and standard deviations were also analyzed. Additionally, Pearson's Correlation Coefficient was used to analyze the survey results to determine if there was a significant relationship between the variables in the survey and ANOVA was implemented to find significant differences in mean PCS Scores and the Amount of Training Received Category.

Summary

Quantitative data on the perceived confidence, compliance commitment, and sustainability ratings for RMF were collected and used in this research. The independent variable is RMF Training, and the dependent variables are RMF effectiveness, RMF sustainability, and RMF commitment. A survey questionnaire was distributed utilizing Perceived Competence Scales (PCS) to assess the degree in which participants felt confident in RMF effectiveness, RMF commitment, and RMF sustainability in relation to receiving formal RMF training. The questionnaire was presented to the LinkedIn group titled Risk Management Framework (RMF) Resources Center. The research has been evaluated for ethical factors and no PHI or PHI was collected for the research and all

ethical baselines in maintaining research integrity and validity were being considered. Data were analyzed utilizing descriptive statistics including means and standard deviations and the Pearson correlation coefficient.

CHAPTER FOUR

FINDINGS

Overview

This chapter presents research findings, including an evaluation of data and summary of the study's conclusions. The purpose of this quantitative research was to investigate the associations between formal RMF training and the perceptions of RMF effectiveness, RMF commitment, and RMF sustainability in RMF practitioners. A questionnaire based on Perceived Competency Scales (PCS) was disseminated to RMF practitioners to collect their responses on the amount of formal RMF training received as well as perceptions of RMF effectiveness, RMF commitment, and RMF sustainability.

The survey was presented to RMF practitioners who were members of a LinkedIn group titled Risk Management Framework (RMF) Resource Center. The Group Owner of the Risk Management Framework (RMF) Resource Center provided approval for the study (See Appendix C). Members of the group were also sent private messages with a survey invitation and link. A total of 200 private messages were sent via LinkedIn messenger with a response rate of 81 students completing the survey.

The survey consisted of a validated instrument for measuring perceived competence consisting of Likert-type scales which were used to measure perceptions of RMF effectiveness, RMF commitment, and RMF sustainability. In addition, the participants were asked how much formal RMF training they had received and if they had any additional comments on RMF effectiveness, RMF commitment, and RMF sustainability. An introductory paragraph described the research study and informed

consent was offered to the participants for acceptance. The survey was made available for seven days and delivered via Survey Monkey.

Data Recording

The survey consists of three sections which are based on Likert-type scales, each consisting of four statements about the participant's confidence in RMF effectiveness, RMF commitment, and RMF sustainability. In order to conduct ANOVA statistical analysis and Pearson's Correlations, the four PCS statements were scored and then evaluated in relation to the Amount of Training Received Category. The PCS Score was obtained by calculating the average responses on the four statements (Deci, 2006). The Amount of Training Received Category was organized by hours of training divided into Low (0-32), Moderate (32-40), and High (40+). Specifically, ANOVA was used to determine if any statistically significant differences existed between mean PCS Scores and the Amount of Training Received Category. Descriptive statistics including means and standard deviations were also analyzed. Additionally, Pearson's Correlation methods were used to analyze the survey results to determine if there was a significant relationship between correlations of PCS Scores and the Amount of Training Received Category.

The calculation of the Cronbach's alpha score was used to establish validity for the PCS. Cronbach's alpha scores assess reliability and measures of the degree in which instruments reflect stability (Cooper & Schindler, 2016). In this study, the Cronbach's alpha score was .952 for the RMF Effectiveness PCS (see Table 1), .944 for the RMF Commitment PCS (see Table 2), and .961 for the RMF Sustainability PCS (see Table 3). The three scales are therefore acceptable as .70 or higher is deemed valid (Cortina, 1993).

Table 1.

Cronbach's Alpha: Effective PCS

Case Processing Summary

		N	%
Cases	Valid	81	100.0
	Excluded[a]	0	.0
	Total	81	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.952	4

Table 2.

Cronbach's Alpha: Commitment PCS

Case Processing Summary

		N	%
Cases	Valid	81	100.0
	Excluded[a]	0	.0
	Total	81	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.944	4

Table 3.

Cronbach's Alpha: Sustainability PCS

Case Processing Summary

		N	%
Cases	Valid	81	100.0
	Excluded[a]	0	.0
	Total	81	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.961	4

Findings

Table 4 presents descriptive statistics of the Amount of Training Received Category, Training Hours Received, and PCS Scores. From Table 4, it can be observed that the Amount of Training Received was split into the categories of 1-3 with Category 1 indicating a low threshold of RMF training hours received and Category 3 indicating the receipt of a high threshold of RMF training hours received. The mean of training being 2.32 suggests that most RMF practitioners who participated in this study had received intermediate to advanced formal RMF training. Training hours ranged from 0 hours to the most advanced participants with 160 hours demonstrating a wide range of RMF training education hours. The mean training hours received was 44.57 which suggested the majority of students received one week of RMF training which is the most common RMF training duration offered (Berman, 2018). In approaching PCS Scores, it is evident that the minimum rates for the Effective PCS came in much higher than Commitment PCS

and Sustainability PCS at 2.00. The mean data point for Commitment PCS presented the highest rating of 5.8488 with the lowest consistent rating being the Sustainability PCS Score 5.0988. Overall, the data presented a broad well-balanced range of collection and distribution.

Table 4.

Descriptive Statistics

Descriptive Statistics

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Variance
Amount of Training Received Category	81	2	1	3	2.32	.788	.621
TrainingHoursReceived	81	160	0	160	44.57	34.333	1178.723
Effective PCS Score	81	5.00	2.00	7.00	5.7685	1.25547	1.576
Commitment PCS Score	81	5.25	1.75	7.00	5.8488	1.21878	1.485
Sustainability PCS Score	81	6.00	1.00	7.00	5.0988	1.60258	2.568
Valid N (listwise)	81						

An analysis of variance (ANOVA) was utilized to establish if statistically significant data existed between the means of PCS Scores and Amount of Training Hours Received Category. The results of the ANOVA showed that there was a significant difference in the mean Effective PCS Scores among those with varied levels of formal RMF training (MS = 5.388), (F [2,78] = 3.645, $p < .05$) (see Table 5 and Figure 3). Upon additional analysis using the post-hoc Duncan's Multiple Range Test a significant difference appeared between Training Received Category 2 and Training Received Category 3 in relation to Effective PCS Scores (see Table 6). No significant difference was found between the means of Commitment PCS Scores and the Training Received Category (MS = 3.210), (F [2,78] = 2.227, $p >. 05$) or Sustainability PCS Scores (MS = .296), (F [2,78] = .113, $p >. 05$) (see Table 5, Figure 4, and Figure 5).

Table 5.

ANOVA: PCS by Training Hours Categories

ANOVA

		Sum of Squares	*df*	Mean Square	*F*	Sig.
Effective PCS Score	Between Groups	10.777	2	5.388	3.645	.031
	Within Groups	115.321	78	1.478		
	Total	126.097	80			
Commitment PCS Score	Between Groups	6.420	2	3.210	2.227	.115
	Within Groups	112.415	78	1.441		
	Total	118.835	80			
Sustainability PCS Score	Between Groups	.592	2	.296	.113	.893
	Within Groups	204.867	78	2.627		
	Total	205.460	80			

Table 6.

Duncan's Multiple Range Test

Effective PCS Score

Duncan[a,b]

Amount of Training Received		Subset for alpha = 0.05	
Category	*N*	1	2
2	23	5.3587	
1	16	5.4375	5.4375
3	42		6.1190
Sig.		.826	.060

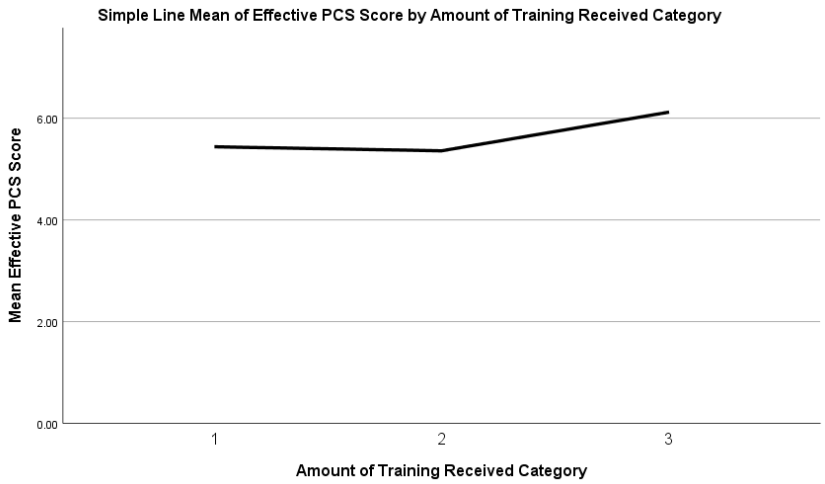

Figure 3. Simple Line Mean of Effective PCS Score by Amount of Training Received Category.

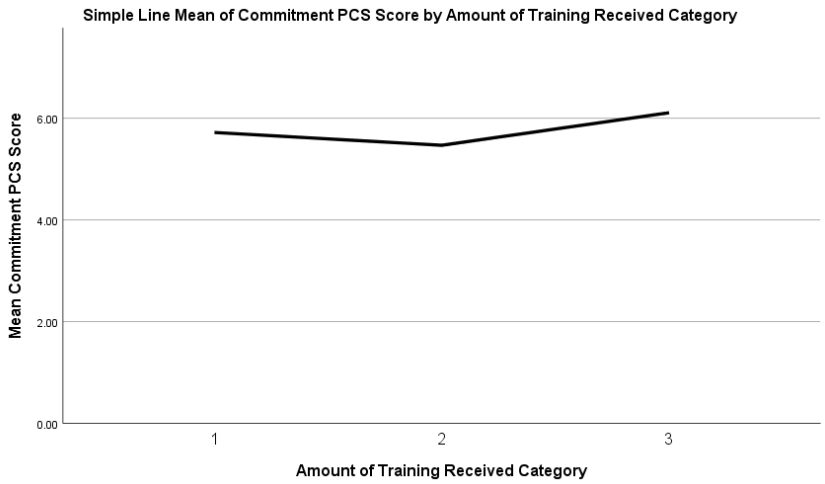

Figure 4. Simple Line Mean of Commitment PCS Score by Amount of Training Received Category.

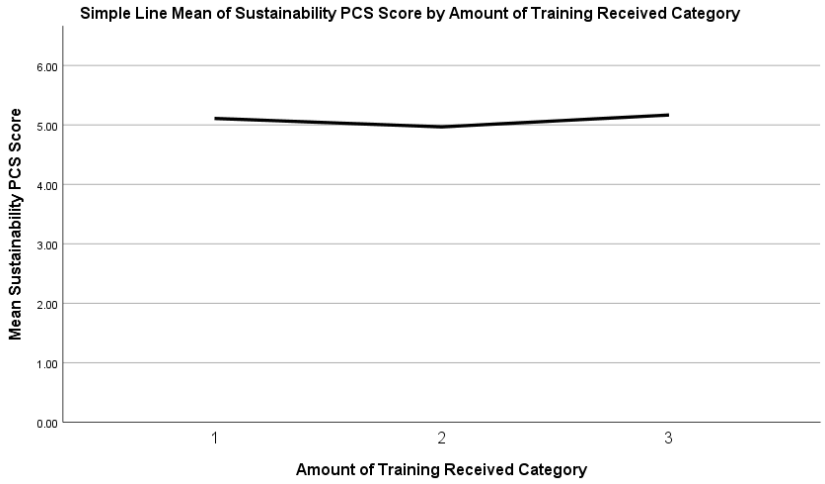

Figure 5. Simple Line Mean of Sustainability PCS Score by Amount of Training Received Category.

Correlation analyses were conducted to explore the relationships between PCS Scores and the Amount of Training Received Category. Pearson's Product-Moment Correlation Coefficient *(r)* analysis was used for this purpose due to the test's measurement of the strength of linear relationship between variables with an objective of establishing initial causality signals (Spatz, 2011). The value of r can vary from -1.0 to +1.0 with the sign indicating the directions relationship. Statistical significance for the Pearson's Product-Moment Correlation Coefficient *(r)* is reported in Table 7 which shows a correlation summary table.

Table 7.

Correlation Summary Table

Correlations

		Amount of Training Received Category	Effective PCS Score	Commitment PCS Score	Sustainability PCS Score
Amount of Training Received Category	Pearson Correlation	1	.253*	.168	.027
	Sig. (2-tailed)		.023	.133	.814
	N	81	81	81	81
Effective PCS Score	Pearson Correlation	.253*	1	.708**	.541**
	Sig. (2-tailed)	.023		.000	.000
	N	81	81	81	81
Commitment PCS Score	Pearson Correlation	.168	.708**	1	.593**
	Sig. (2-tailed)	.133	.000		.000
	N	81	81	81	81
Sustainability PCS Score	Pearson Correlation	.027	.541**	.593**	1
	Sig. (2-tailed)	.814	.000	.000	
	N	81	81	81	81

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Results of the Pearson's Correlation indicated that there was a significant positive association with the Effective PCS Score and the Amount of Training Received Category, (r = .253, n = 81, p = .023). The Commitment PCS Score showed weak positive correlation (r = .168). Similarly, the correlation Sustainability PCS Score showed the weakest correlation (r = .027). Scatterplots of correlations can be found in Figure 6, Figure 7, and Figure 8.

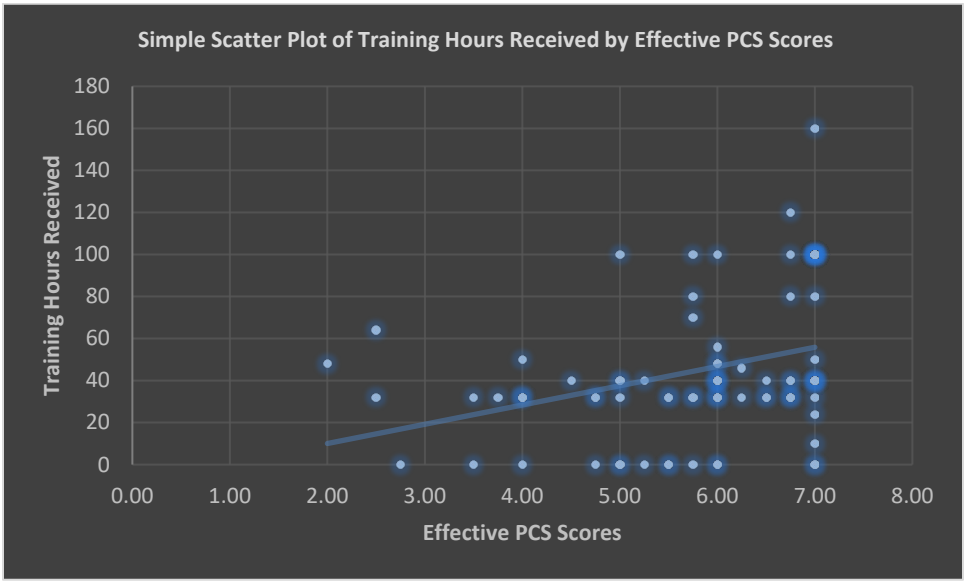

Figure 6. Simple Scatter Plot of Training Hours Received by Effective PCS Scores.

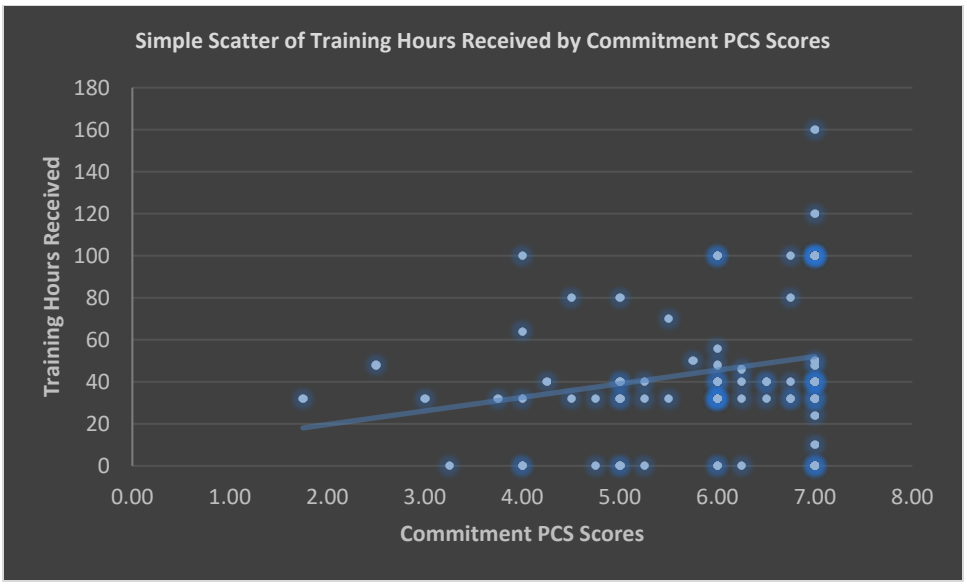

Figure 7. Simple Scatter Plot of Training Hours Received by Commitment PCS Scores.

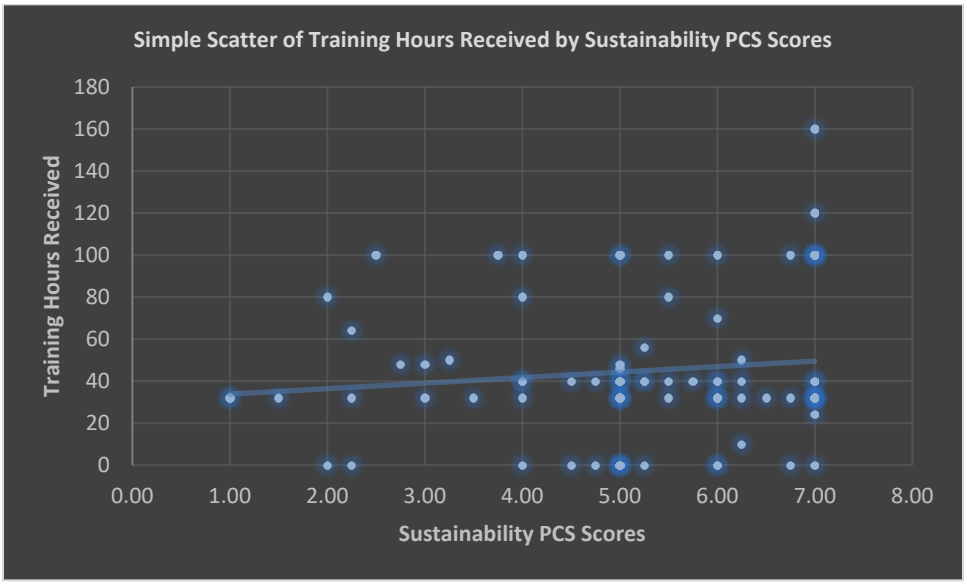

Figure 8. Simple Scatter Plot of Training Hours Received by Sustainability PCS Scores.

Responses to open-ended questions are in Appendix E. Frequency analysis tables can be found in Appendix F.

Analysis and Evaluation of Findings

Hypothesis 1 – RMF Effectiveness

RMF practitioners who have received formal RMF training will perceive RMF as being effective in protecting the U.S. Government's technology infrastructure.

H_0: There is no relationship between receiving RMF training and a positive perception of RMF effectiveness.

H_1: There is a relationship between receiving formal RMF training and a positive perception of effectiveness.

A significant positive relationship exists between receiving formalized RMF training and the perception of RMF effectiveness as shown by the results of Pearson's Correlation, ($r = .253$, $n = 81$, $p = 023$). ANOVA supports this relationship as shown by significant difference in the mean Effective PCS Scores among those with varied levels of formal RMF training (MS = 5.388), (F [2,78] = 3.645, $p < .05$). Utilizing the post-hoc Duncan's Multiple Range Test range presented a significant difference between Training Received Category 2 and Training Received Category 3 in relation to Effective PCS Scores. Duncan's Multiple Range Test supports these findings showing those with advanced training in Category 3 have a significant positive difference in perceptions of confidence in RMF effectiveness in comparison to Category 2. The null hypothesis that

there is no relationship between receiving RMF training and a positive perception of RMF effectiveness is rejected. Figure 9 illustrates correlation relationships.

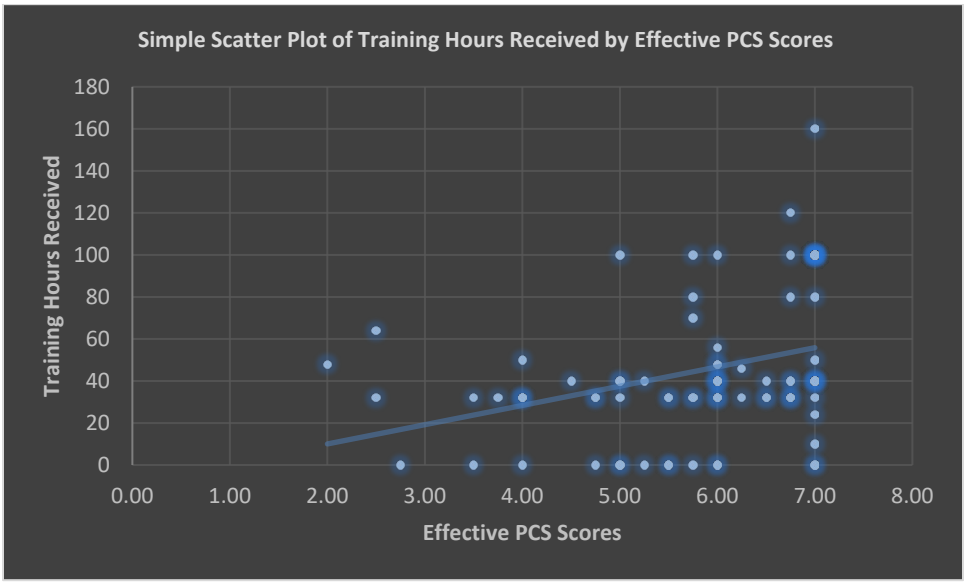

Figure 9. Simple Scatter Plot of Training Hours Received by Effective PCS Scores.

Hypothesis 2 – RMF Commitment

RMF practitioners who have received formal RMF training will display high levels of RMF compliance commitment.

H_0: There is no relationship between receiving formal RMF training and a positive perception of RMF commitment.

H_1: There is a relationship between receiving formal RMF training and a positive perception of RMF commitment.

A weak positive relationship exists between receiving formal RMF training and the perceptions of RMF commitment as shown by the results of Pearson's Correlation, $r = .168$, $n = 81$, $p > .133$. Additionally, ANOVA showed an insignificant difference in the mean Commitment PCS Scores among those with varied levels of training (MS = 3.210), (F [2,78] = 2.227, $p > .115$). The null hypothesis that there is no relationship between

receiving RMF training and a positive perception of RMF commitment is accepted. Figure 10 illustrates the correlation relationship.

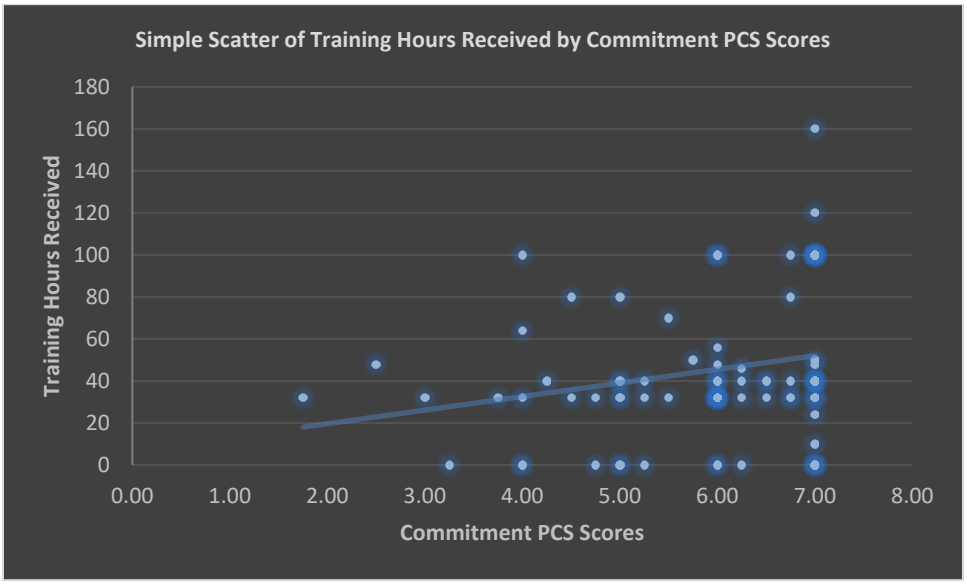

Figure 10. Simple Scatter Plot of Training Hours Received by Commitment PCS Scores.

Hypothesis 3 – RMF Sustainability

RMF practitioners who have received formal RMF training will have confidence that RMF will be a sustainable long-term cybersecurity framework for the U.S. Government.

H_0: There is no relationship between receiving formal RMF training and a positive perception of RMF long-term sustainability.

H_1: There is a relationship between receiving formal RMF training and a positive perception of RMF long-term sustainability.

A weak relationship exists between receiving formalized RMF training and the perceptions of RMF commitment as shown by the results of Pearson's Correlation, $r = .027$, $n = 81$, $p > .814$. ANOVA showed an insignificant difference in the mean

Sustainability PCS Scores among those with varied levels of training (MS = .296), (F [2,78] = .113, p > .893). The null hypothesis that there is no relationship between receiving RMF training and a positive perception of RMF sustainability is accepted. Figure 11 illustrates the correlation relationship.

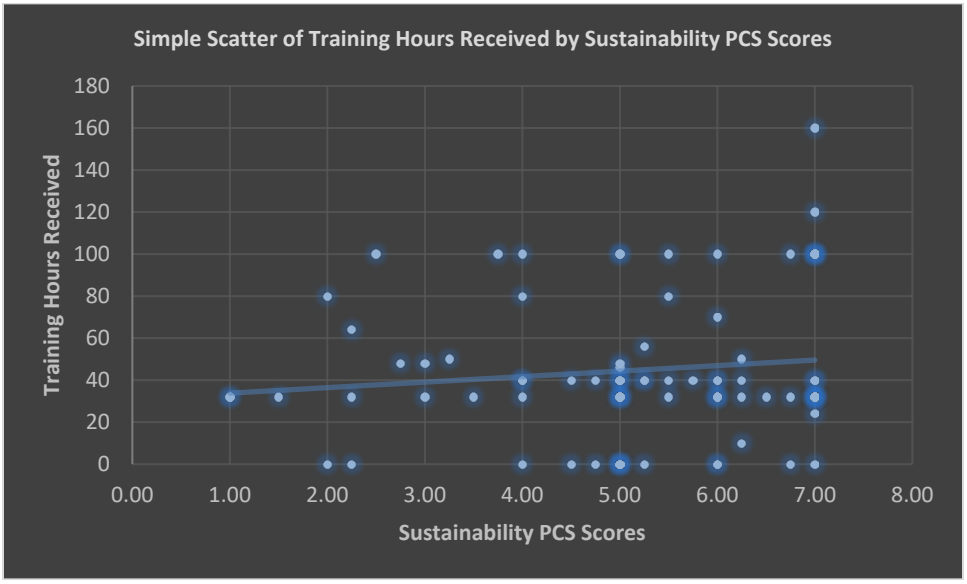

Figure 11. Simple Scatter Plot of Training Hours Received by Sustainability PCS Scores.

Responses to Open-ended Questions

Open-ended questions were included to collect qualitative information from study participants. Due to RMF being comprised of hundreds of pages of intricate U.S. Government policy documentation, it has been observed that RMF practitioners have a wide range of strong opinions and unique interpretations of the topic. Open-ended questions on RMF effectiveness, sustainability, and commitment were discussed. General themes indicated RMF was an expensive process which often lacked support from leadership and government officials. This lack of support was often thought to be from minimal levels of understanding (training) in RMF and a lack of financial resources to

provide required RMF support staff. It could be suggested that through the delivery of high quality RMF training, RMF proficiency could be attained which would create a more efficient RMF support staff potentially reducing overall RMF project costs. Response to open-ended questions can be found in Appendix E.

Summary

The results of data collected in this survey on RMF research are presented in Chapter 4. Data were collected from 81 members of a LinkedIn group titled Risk Management Framework Resource Center. The data were used to gather perceived competency scores of RMF practitioners on the topics of RMF effectiveness, RMF commitment, and RMF sustainability which were statistically evaluated. The PCS responses were converted into PCS Scores which were created by averaging the scores for each scale. The PCS scores were then analyzed in relation to categories of Low, Moderate, and High amounts of training hours received. ANOVA and Correlation analyses were used to explore significance between variables. Statistical significance was established in data collection, but not all relationships established high degrees of statistical significance.

Within the context of the three hypotheses presented, one of three hypotheses were rejected. Pearson's Correlation results indicated a positive significant relationship between perceptions of RMF effectiveness and receiving formal RMF training which rejected the first hypothesis and indicated that receiving formal RMF training has an increase on perceptions of RMF effectiveness. ANOVA supported this conclusion showing significant differences in means for Training Category 2 and Training Category 3 in relation to the Training Hours Received Category which was disseminated by

Duncan's Multiple Range Test. The null hypotheses for the second and third research questions of RMF commitment and RMF sustainability perceptions not being impacted by formal RMF training received were accepted due to significance not being established by means of Pearson's Correlations or ANOVA for the data collected.

CHAPTER FIVE

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

Introduction

U.S. Government information systems are under attack. These attacks are constant and require a robust and effective cybersecurity strategy. RMF is the current cybersecurity framework being implemented by the U.S. Government to strengthen its cybersecurity infrastructure (Graubart & Bodeau, 2016). Those implementing RMF have been struggling with the framework since it was adopted in 2014 via DoDI 8510.01, and there is a growing concern that RMF is broken and that the process is not functioning as intended by the policy writers at NIST (Berman, 2018). Reports of RMF being broken center around RMF being perceived as excessively labor and cost intensive with a concern that it does not make information systems more secure because it is being viewed as a check-the-box paperwork exercise (Maclean, 2017). This study investigated the relationship between receiving formal RMF training and perceptions of RMF Effectiveness, RMF Commitment, and RMF Sustainability. Increased levels of perceived RMF effectiveness, RMF commitment, and RMF sustainability would potentially offset concerns of RMF failing in its mission. This research was viewed as necessary due to very minimal previous research being conducted on RMF and no previous research on the relationships between perceived RMF effectiveness, perceived RMF commitment, and perceived RMF sustainability in relation to the receipt of formal RMF training. RMF experts have indicated that formal RMF training is necessary for RMF practitioners to have a thorough understanding of the RMF process (Berman, 2016).

The results of the study showed statistically significant correlations between RMF practitioners receiving formal RMF training and increased perceptions of RMF effectiveness. Those who were categorized as receiving the most RMF training (40+ hours) exhibited the highest increase in levels of perceived RMF effectiveness. Overall perceptions of RMF effectiveness showed a consistent increase across each category of RMF training received (low, medium, high) with the biggest increase with RMF practitioners who had received the highest level of RMF training hours.

A statistically significant relationship between RMF practitioners' perceptions of RMF commitment and the amount of formalized RMF training received by RMF practitioners could not be established. Additionally, a statistically significant relationship between RMF practitioners' perceptions of RMF sustainability and RMF practitioners' receipt of formalized RMF training could also not be established. Weak relationships between perceptions of RMF commitment and the recipient of formalized RMF were observed, although they were not statistically significant.

Discussion of Findings

Risk Management Framework (RMF) Effectiveness

Hypothesis 1 – RMF practitioners who have received formal RMF training will perceive RMF as being effective in protecting the U.S. Government's technology infrastructure.

This hypothesis was accepted. RMF practitioners who reported receiving the highest amount of formal RMF training hours also showed increased levels of perceptions of RMF effectiveness. Respondents who had received more than 40 hours of formal RMF training reported the highest perceptions of RMF effectiveness.

RMF practitioners without formal RMF training lack a thorough understanding of RMF due to cognitive overload caused by the hundreds of pages of NIST policy documentation which outline RMF. Formalized RMF training breaks this information into smaller more manageable pieces of data increasing the learners understanding of the RMF process. These findings are supported by Cognitive Load Theory which suggests breaking information into smaller pieces reduces cognitive load and increases the learner's processing of information (Nesvig, 2014). By learners having increased levels of knowledge processing, their perceptions of RMF effectiveness are increased due to their enhanced understanding of the RMF process. These findings are echoed by RMF subject matter experts who have indicated that RMF is wrought with a staggering amount of policy guidance which overwhelms those trying to learn the process (MacLean, 2016).

Risk Management Framework (RMF) Commitment

Hypothesis 2 – RMF practitioners who have received formal RMF training will display high levels of RMF compliance commitment.

This hypothesis was rejected. RMF practitioners who reported receiving the highest amount of formal RMF training hours did not show a significant increased level of perception of RMF commitment. A weak increase in perceptions of RMF training commitment and receiving formal RMF training emerged from data collection, but the results were not statistically significant. Future research with a larger sample size could magnify the weak correlations shown by this study.

These findings align weakly with Social Exchange Theory. Social Exchange Theory operates on a cost and reward basis suggesting RMF practitioners would have an

increased commitment to the RMF process due to the time and financial commitment their organization invested in them (Ehrhardt, Miller, Freeman, & Hom, 2011). Although statistically significant relationships between perceptions of RMF commitment and the receipt of formalized RMF training could not established in this study, the author is confident a larger sample size would have altered this outcome. This observation is rooted in the upward trend shown in Figure 7 as well as the results of ANOVA and Correlation statistical analyses being close to statistically significant. Beyond Social Exchange Theory, specific literature supporting increased RMF commitment in relation to the receipt of formalized RMF training was not found.

Risk Management Framework (RMF) Sustainability

Hypothesis 3 – RMF practitioners who have received formal RMF training will have confidence that RMF will be a sustainable long-term cybersecurity framework for the U.S. Government.

This hypothesis was rejected. RMF practitioners who reported receiving the highest amount of formal RMF training hours did not show an increased level of perceptions of RMF sustainability. As shown by Figure 11. Simple Scatter Plot of Training Hours Received by Sustainability PCS Scores, no significant trend of increase or decrease in the perceptions of RMF sustainability and the receipt of formal RMF training could be established. The lowest perceptions of RMF sustainability were reported from those who had received 30 – 40 hours of RMF training and the highest

overall sustainability rankings were from those in the most advanced training category of 40+ hours.

As suggested in Bloom's Taxonomy, it was theorized that an increased level of cognitive mastery relating to the RMF process would result in increased levels of the perception of RMF sustainability. The findings of this study did not align with theoretical assumptions in literature related to Bloom's Taxonomy. Unlike the other two dependent variables of RMF effectiveness and RMF commitment, the variable of RMF sustainability showed no direct trends or statistical significance in relation to the receipt of formalized RMF training. These results indicate that RMF Practitioners perceptions of RMF sustainability have no relationship with them receiving formalized RMF training. No additional literature on RMF sustainability could be found by the researcher.

Recommendations for Future Research

In future research, it is suggested that alternative cybersecurity frameworks are explored in comparison to RMF. If adjustments are made to RMF based on examining other successful cybersecurity frameworks, RMF practitioners may feel the RMF process is operating in a more effective manner and mitigate the feeling that RMF is a bloated and expensive paperwork exercise.

Larger sample sizes may also be beneficial in further research to explore statistical significance for the dependent variable of RMF commitment in relation to the receipt of formalized RMF training due to the weak positive correlation observed in this research as shown by the results of Pearson's Correlation, $r = .168$, $n = 81$, $p > .133$. A larger sample size could potentially provide a stronger indication of the significance for

this weak positive correlation due to a larger sample size creating a narrower margin of error as well as higher confidence levels (Spatz, 2011).

Summary and Implications of the Study

This research investigated formalized RMF training and the perceptions of RMF effectiveness, RMF commitment, and RMF sustainability. Based on the conclusions of the study and the responses to open-ended questions, some recommendations for future research will be presented to help improve perceptions and implementation of RMF.

It is suggested that the U.S. Government and defense contracting community invest in educational programs that deliver formalized RMF training. This research indicated that RMF practitioners have stronger perceptions of RMF effectiveness when they receive advanced levels of formalized RMF training. It is also suggested that RMF practitioners receive 40+ hours of RMF training to maximize perceptions of RMF effectiveness. RMF is viewed as a time intensive, challenging, and expensive process. In approaching an RMF project with the known obstacles outlined above, maximizing perceived RMF efficiency should greatly reduce time to being granted an Authorization to Operate (ATO) and mitigate possible confusions which lead to projects running into delays from a time management perspective. RMF must be a holistic process and not just seen as a paperwork exercise. While RMF guidance documents reiterate this concept, RMF practitioners may not understand this until they receive formal RMF training.

It is highly suggested that executive leadership receive a baseline of formal RMF training. RMF is a complicated process which is plagued with potential issues and

shortfalls. Gaining executive commitment and a thorough understanding of the RMF process will assist with proper RMF project funding and leadership fully understanding the challenges RMF presents. It is understood that those in executive leadership positions are very busy and often cannot take the time to fit formal training in their schedule. Taking the nature of these executives' roles into consideration, a one-day RMF fundamentals class would be a good start in training executive leadership in RMF. Once RMF leadership understands the nuances and workforce requirements of RMF, the issues of RMF having a lack of funding and executive commitment are potentially mitigated as these issues may come from a lack of understanding in the complexity of the RMF process.

DoD must publish guidance for policies and procedures as well as support tools for Continuous Monitoring. RMF packages are not being maintained in a capacity that can be leveraged to make the process of evaluating systems for continued ATO in three year increments effective. Due to a lack of DoD guidance in Continuous Monitoring, RMF teams are often receiving their ATO's and then putting their RMF packages on the shelf until their ATO's expire in the requisite three-year timeframe. If DoD were to publish clear Continuous Monitoring guidance, RMF teams would be better prepared for reauthorization and the overall cybersecurity status of their information systems would be better due to the system being continuously monitored after the receipt of an ATO and not just forgotten about.

Additional recommendations are drawn from the open-ended survey question which asked if survey participants had any additional comments regarding their perception of RMF effectiveness, sustainability, or commitment as it relates to receiving

formal RMF training. The most common repetitions in these responses referenced a lack of leadership commitment, a need for DoD to provide clear guidance regarding the application of continuous monitoring, and a lack of manpower.

With the threat landscape and criticality of U.S. Government information systems, it is unacceptable to view RMF as a meaningless check-the -box compliance process that is quickly put on a shelf once an ATO is achieved. It is the authors hope that the U.S. Government does not experience events which lead to losses of life and catastrophic tragedies before RMF is taken seriously.

REFERENCES

Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for NIST Cyber Security Framework (pp. 51–62). Academy & Industry Research Collaboration Center (AIRCC). https://doi.org/10.5121/csit.2017.70305

Assi, Carol. (2018, April 30). Fort Belvoir - CIO/G6 Office Interview [personal interview].

Benamati, J., & Lederer, A. L. (2001). Coping with rapid changes in IT. Communications of the ACM, 44(8), 83-88. https://doi:10.1145/381641.381664

Berman, Lon. (2018). Is RMF Broken? Can it be fixed or is it beyond repair? Risk Management Framework Today, 8, 4.

Berman, Lon. (2016). RMF Pitfalls. Risk Management Framework Today, 6, 3.

Blake, James. (2018, June 2). Raytheon – RMF Professional [personal interview].

Bond, P. J. (2004). Standards for Security Categorization of Federal Information and Information Systems - FIPS 199, 13.

Bryce, H. (2017). The Internet of Things Will Be Even More Vulnerable to Cyber Attacks. from https://www.chathamhouse.org/expert/comment/internet-things-will-be-even-more-vulnerable-cyber-attacks

Chung, J. J. (2018). Critical Infrastructure, Cybersecurity, and Market Failure. *Oregon Law Review*, *96*, 36.

Cohen, J. (1992). A power primer. Psychology Bulletin, 112(1), 155-159

Committee on National Security Systems (CNSS) Instruction No. 4009 (2015). Committee on National Security Systems (CNSS) Glossary. Retrieved from https://www.cnss.gov/CNSS/issuances/Instructions.cfm

Cooper, D. R., & Schindler, P. S. (2006). *Business research methods* (9th ed.). New York: McGraw-Hill.

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. Journal of applied psychology, 78(1), 98.

Creswell, J. W. (2013). Research Design. Thousand Oaks: SAGE Publications.

Cyber Incident & Breach Trends Report (2018). Online Trust Alliance (OTA). Retrieved from https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

Daily, K. (2017). RMF: Is It Effective? Retrieved from https://www.itdojo.com/rmf-is-it-effective/

Deci, E. L. (2006). Perceived competence scales. Retrieved July 15, 2018, from http://www.psych.rochester.edu/SDT/measures/comp.html

Dempsey, K. L., Chawla, N. S., Johnson, L. A., Johnston, R., Jones, A. C., Orebaugh, A. D. (2011). Information Security Continuous Monitoring (ISCM) for federal information systems and organizations (No. NIST SP 800-137). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137

Department of Defense. (2014). Risk Management Framework (RMF) for DoD Information Technology (IT), (8510.01). Retrieved from https://fas.org/irp/doddir/dod/i8510_01.pdf

Duffy, J., & McDonald, J. (2015). Technology and learning. In Teaching and learning with technology (Fifth ed.). Pearson.

Ehrhardt, K., Miller, J. S., Freeman, S. J., & Hom, P. W. (2011). An examination of the relationship between training comprehensiveness and organizational commitment: Further exploration of training perceptions and employee attitudes. Human Resource Development Quarterly, 22(4), 459-489. doi:10.1002/hrdq.20086

Federal Information Security Modernization Act of 2002, Pub. L. No. 107–347 (Title III) (2002). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283 (2014). Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

Ford, N. (2018). Blended Learning: Why It Is Important to Mix It Up. Retrieved from https://www.skillsoft.com/blog/2018/03/blended-learning-why-it-is-important-to-mix-it-up/

Graubart, R., & Bodeau, D. (2016). The Risk Management Framework and Cyber Resiliency, 13. Retrieved from https://www.mitre.org/publications/technical-papers/the-risk-management-framework-and-cyber-resiliency

Guidelines for Computer Security Certification and Accreditation (No. FIPS 102) (1983). National Bureau of Standards.

Gyenes, R. (2014). A Voluntary Cybersecurity Framework Is Unworkable - Government Must Crack the Whip. *Pittsburgh Journal of Technology Law and Policy*, *14*(2), 293–314. https://doi.org/10.5195/TLP.2014.146

Heick, T. (2017). What Is the Cognitive Load Theory? A Definition for Teachers -. Retrieved from https://www.teachthought.com/learning/cognitive-load-theory-definition-teachers/

Hussain, W. (2017). Risk Management Framework to Avoid SLA Violation in Cloud from a Provider's Perspective. Center for Applied Cybersecurity Research.

Jackson, C. (2017) Beyond the Beltway the Problems with NIST's Approaches to Cybersecurity. Center for Applied Cybersecurity Research.

Joint Task Force Transformation Initiative. (2004). Guide for the Security Certification and Accreditation of Federal Information Systems (No. NIST SP 800-37). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r1

Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (No. NIST SP 800-30r1). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Joint Task Force Transformation Initiative. (2014). Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach (No. NIST SP 800-37r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r1

Joint Task Force Transformation Initiative. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (No. NIST SP 800-37 Rev 2 (DRAFT). National Institute of Standards and Technology.

Kissel, R. (2013). Glossary of key information security terms (No. NIST IR 7298r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7298r2

Kohnke, A., Sigler, S., Shoemaker, D. (2016). Strategic Risk Management Using the NIST Risk Management Framework, EDPACS The EDP Audit, Control, and Security Newsletter *53*(5).

Leonard, A. (2015). Top Ten—Data Breaches that Made the News. Risk Management Framework Today, 5, 3.

Maclean, D. (2017). The NIST Risk Management Framework: Problems and recommendations. *Cyber Security: A Peer-Reviewed Journal*, 1(3), winter 2017, 207-217(11)

Managing Information as a Strategic Resource (OMB Circular No. A-130). (2016), 19.

McHaney, Roger. (2011). The New Digital Shoreline. Sterling, VA: Stylus Publishing, LLC.

Metheny, M. (2013). Applying the NIST Risk Management Framework. Federal Cloud Computing, 103-167. doi:10.1016/b978-1-59-749737-4.00005-8

National Institute of Standards and Technology. (2004). Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD: National Institute of Standards and Technology

National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (No. NIST Cybersecurity White Paper). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.02122014

Nesvig, B. (2014, June 12). The Power of Chunking: How To Increase Learning Retention. Retrieved from https://www.dashe.com/blog/learning/chunking-memory-retention/

Nevid, J. S. (2012). Classes in Bloom: Integrating blooms taxonomy in the classroom. PsycEXTRA Dataset. doi:10.1037/e669402012-019

NICCS. (2017). National Cyber Security Awareness Month. Retrieved from https://niccs.us-cert.gov/featured-stories/national-cyber-security-awareness-month-2017

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security (No. NIST SP 800-12r1). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017). Retrieved from https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Public Law 113–274, Pub. L. No. 128 STAT. 2971. (2014). Retrieved from https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf

Shackelford, S. J. (2016). Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks. *UC Davis Business Law Journal*, 16-2

Shackleford, S., Proia, A., Martell, B., & Craig, A. (2014). Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices, *Texas International Law Journal*

Shen, L. (2014). The NIST Cybersecurity Framework: Overview and Potential Impacts, *SciTech Lawyer,* 10-4

Smith, L. (2018). Perceived RMF Weakness. Risk Management Framework Working [personal interview].

SolarWinds Federal Cybersecurity. (2017). SolarWinds Federal Cybersecurity Survey 2017: Government Regulations, IT Modernization, and Careless Insiders Undermine Federal Agencies' Security Posture. Retrieved from https://www.slideshare.net/SolarWinds/solarwinds-federal-cybersecurity-survey-2017-government-regulations-it-modernization-and-careless-insiders-undermine-federal-agencies-security-posture/1

Spatz, C. (2011). Basic Statistics: Tales of Distributions. Australia: Wadsworth.

Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., & Gulick, J. (2008). Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, 53.

Stine, K., Kissel, R., Barker, W. C., Lee, A., & Fahlsing, J. (2008). Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, 304.

Tran, J. L. (2015). Navigating the Cybersecurity Act of 2015, *Chapman Law Review, 19*

Webb, N. (2015). Why NIST's Free Online RMF Training is Not Enough. Retrieved from https://www.itdojo.com/why-nists-free-online-rmf-training-is-not-enough.

Williams, G. C., Freedman, Z. R., & Deci, E. L. (1998). Supporting autonomy to motivate glucose control in patients with diabetes. *Diabetes Care, 21,* 1644-1651.

Appendices

Appendix A

Invitation to Participate in a Survey

LinkedIn Group
Risk Management Framework RMF Resource Center

Dear participants;

I am a Ph.D. Candidate at University of the Cumberlands. I am working toward my Ph.D. in Information Technology with specialization in Cybersecurity. I am writing this letter to provide information and request your consent to gather data from you regarding your assessment of Risk Management Framework (RMF).

The purpose of this investigation and survey research is to determine how the amount of formal RMF training one receives relates to confidence ratings in RMF effectiveness, RMF compliance commitment, and the long-term sustainability of RMF as a cybersecurity framework for the U.S. Government. This study can provide a better understanding of the need for additional training resources for RMF in the U.S. government and private sector. This research is intended to be used as a resource for leadership and administrators in government agencies as well as the contractor community to aid and guide in the training policy development process for RMF education with the end goal of creating a coherent understanding of RMF and proper application.

The results of this survey will be analyzed. Participants names and other personal information such as emails will not be requested, collected, analyzed or displayed in any part of the research.

The research study poses no apparent risks to the participants. Participation is voluntary. No identifying information will be collected or reported in the research findings.

Sincerely,

P. Devon Schall, Ph.D. Candidate
School of Computer and Information Sciences, University of the Cumberlands
E-Mail: pschall5712@ucumberlands.edu
Tel: 540-327-1772

Appendix B

Informed Consent Form

SURVEY CONSENT – AGREEMENT

I volunteer to participate in an online research survey conducted by doctoral candidate, P. Devon Schall, at University of the Cumberlands. This data collected will be analyzed and written as part of a dissertation research project. Results of this study may be published or released in professional journals, however, no personal or identifying information will be collected or released.

1. My participation in this project is voluntary. I understand that I will not be paid for my participation. I may withdraw and discontinue participation at any time without penalty. If I decline to participate or withdraw from the survey, no punitive action will be taken.

2. I understand that most participants may find the survey interesting and thought-provoking. If, however, I feel uncomfortable in any way, I have the right to decline to answer any question or to end the survey.

3. Participation involves answering questions to an online survey. The survey will last approximately 7-10 minutes.

4. I understand that the researcher will not identify me by name in any reports using information obtained from the survey, and that my confidentiality as a participant in this research project will remain secure. Subsequent uses of records and data will be subject to standard data use policies, which protect the anonymity of individuals and institutions.

5. Data collected as part of the survey is being collected with permission from the instruments original authors and may be shared and published as part of the dissertation process, however, no identifying personal information will be asked, gathered or shared.

6. I understand that this research study has been reviewed and approved by the Institutional Review Board (IRB) for Studies Involving Human Subjects.

7. I have read and understand the explanation provided to me. I have had all my questions answered to my satisfaction, and I voluntarily agree to participate in this study.

8. I acknowledge consent for participation and agree to participate in this research project by making the decision to participate in the survey

Please contact me for any further information, questions, or concerns.

Sincerely,

P. Devon Schall, Ph.D. Candidate
School of Computer and Information Sciences, University of the Cumberlands
E-Mail: pschall5712@ucumberlands.edu
Tel: 540-327-1772

Appendix C

Community Partner Cooperation Letter

P. Devon Schall
University of the Cumberland

Mr. Schall,

Please accept this letter as an acknowledgment of consent for you to utilize the LinkedIn group Risk Management Framework Resource (RMF) Center as a platform for survey collection for your study on the RMF.

I currently serve as Group Owner of this entity, and I am excited in participating in your study on RMF.

Please contact me for any further information, questions, or concerns.

Sincerely,

Kathryn Daily, CISSP
Executive Director
RMF Resource Center

Executive Director of Technical and Consulting
Services kathryn@rmf.org

Appendix D

Research Instrument

Perceived Competence Scales (PCS)

Scoring Information. This scale has 4 items, and an individual's score is simply the average of his or her responses on the 4 items.

Perceived Competence (RMF Effectiveness)

Please indicate the extent to which each statement is true for you, assuming that you received formal RMF training. Use the following scale:

1	2	3	4	5	6	7
not at all true			somewhat true			very true

1. I feel confident in my ability to be effective in performing the RMF process.
2. I now feel capable of performing the RMF process.
3. I am able to perform the RMF process.
4. I am able to meet the challenge of performing the RMF process.

Perceived Competence (RMF Commitment)

Please indicate the extent to which each statement is true for you, assuming that you received formal RMF training. Use the following scale:

1	2	3	4	5	6	7
not at all true			somewhat true			very true

1. I feel confident in my commitment to the RMF process.
2. I now feel capable of being committed to the RMF process.
3. I am able to have commitment to the RMF process.
4. I am able to meet the challenge of being committed to the RMF process.

Perceived Competence (RMF Sustainability)

Please indicate the extent to which each statement is true for you, assuming that you received formal RMF training. Use the following scale:

1	2	3	4	5	6	7
not at all true			somewhat true			very true

1. I feel confident in RMF being a sustainable cybersecurity framework for the U.S. Government.
2. I now feel RMF is capable of being a being a sustainable cybersecurity framework for the U.S. Government.
3. I am able to believe that RMF is capable of being a being a sustainable cybersecurity framework for the U.S. Government.

4. RMF is able to meet the challenge of being a sustainable cybersecurity framework for the U.S. Government.

Open-Ended Questions

Do you have any additional comments regarding your perception of RMF effectiveness, sustainability, or commitment as it relates to receiving formal RMF training?

How much formal RMF training have you received?

Appendix E

Responses to Open-Ended Questions

Do you have any additional comments regarding your perception of RMF effectiveness, sustainability, or commitment as it relates to receiving formal RMF training?

1. The RMF framework is a valuable resource. The checklist items include things that not everyone would notice, expect, guard against. RMF suffers a bad reputation because some government agencies "over-do" it and interpret it literally rather than pragmatically. Also, the govt mandated tools are (no surprise) mediocre, not best-of-breed. A need for continuous monitoring guidance is necessary.

2. I believe this is a great framework so far. Hopefully it will sustain itself for future technology and not change drastically.

3. RMF will require some effort/work factor. Well written/well-meaning business rules, process guides, and continuous monitoring step by step instruction are meant to be used - not ignored!

4. The timeline of an expected RMF ATO is highly skewed in theory vs practice. The overhead is exponential. The benefit of RMF is negligible over DIACAP ATO.

5. Seems so labor intensive and is growing. That is the concern.

6. The implementation of RMF in the US Gov through eMASS has greatly increased the work load of the process. The other huge issue is that parts of RMF processes (ex..Continuous Monitoring) has not be defined as to how they want it done. The inherited controls and CCI's in eMASS should have been completed first and pushed to all projects.

7. I believe RMF training is critical for all security practitioners working within the US Government in order for them to have an understanding of the importance of the process and especially sustaining process.

8. The biggest problem we have had with RMF is working with the DOD who also is new to the RMF process. Some issues include using EMASS and our site not having SIPRNET on sight to gain access to EMASS. The other issue we ran into is when our company would come up with the CIA of the system and our customers want to change that. We ran into an issue of continuous monitoring being unclear.

9. Heavy lack of manpower to effectively complete and sustain RMF is a key contributing factor. The US Government is too slow to adapt to such a process like RMF in order to make it successful.

10. Yes- This all comes from the assumption that there will be willingness on the governments part to participate. We have all been given the skills and can probably do it to the best of our ability- but government leadership can stop all actions of completing an RMF package.

11. Several loopholes that needs to be addressed. Civilian agencies and the Military agencies should not be on the same framework.

12. Since most systems are built by contractors the RMF process should be performed during the contracting process. But RMF is too expensive.

13. Training effectiveness will depend GREATLY upon the qualitative interpretation of the governing agencies' auditors. RMF, as a "perceived risk approach" is not a black and white exercise and has the potential for greatly exaggerated differences between auditors.

14. It would be useful to see more attention given to the human side of the RMF, e.g.: a guidance and official policy on identifying and assigning stakeholders to roles, methods and tools for determining 'who' to talk to and a more refined approval chain.

15. I believe it works only with full cooperation from government.

16. As for sustainability I would like to work on a few projects prior to answering this honestly.

17. My perception is that the gov't is still working out its own internal RMF processes and requirements, such that it challenges the sustainability of the process, and creates a delta between what is taught in training and what is experienced in working through the RMF process.

18. I believe that the individuals receiving classroom training on RMF will be able to be effective in their development and execution of an RMF package. However, because many of the managers have not attended training, commitment and sustainability are going to be a challenge because the workforce may not have the resources needed to be effective - i.e. time, people, money. If management does not also support the continuous monitoring process the entire concept of RMF is in jeopardy. System Owners are ultimately the responsible party for the execution

of a successful RMF package as well as Continuous Monitoring, and yet those individuals rarely attend RMF training classes.

19. RMF has the capability of being usable for the foreseeable future within the DoD, the issue is there are too many upper level people making decisions that do not have a concept of how to use it. Unnecessary additional levels of oversight have been created within deferent branches of the military that don't add anything to the process but just give someone a job. Way too much is left up to individual interpretation. Assessors can differ greatly on what is acceptable or not

20. Training was fine, the challenge is communicating the multiple implementation process between the federal government, the DoD, non-government

21. RMF will only succeed providing the command continues to support the process.

22. RMF is an effective and sustainable process, when implemented properly. Unfortunately, in the DoD, RMF is simply used as compliance and is usually referred to as DIACAP plus. AOs are still looking for a checkmark, not a true risk assessment. Until that occurs, RMF will not be effective or meet its full potential.

23. Based on current RMF accreditation it appears to me that RMF is a changing. I received training 3 months ago however guidance has already been updated with new requirements/information so at this point I feel RMF is still in its infancy stages.

24. RMF training using trainers with real life experiences made the training experiences much more real and useful.

25. As a commercial enterprise supporting a U.S. Government customer, I believe the formal RMF training I received is baseline effective and sustainable; however, it has inherent limits. These limits are not so much due to training provider shortcomings, but due to the very fragmented nature of the RMF process itself. Granted, the model is a clearly defined six step process that has Risk Acceptance at its core, but it is pinned to a myriad of NIST SPs, DoDIs, DoDMs, CNSSI, and federal regulations. In the case of our ATO process, we rely on >30 of these documents...this makes the model fragmented and open to very broad interpretation or misinterpretation. Formal RMF training, assuming the competency of the trainer is not in question, is effective and sustainable. However, the government and industry need to work towards a model that is more like PCI, COBIT, SOC, and ISO/IEC 27001 if long-term commitment is expected. These models are first and foremost, versioned and vetted by industry. RMF on the other hand, is based on dozens of versions of the aforementioned

documents/regs that often lag behind one another and vetted primarily by the government with wide interpretation by government CIOs and AOs.

26. Support structure is not in place for all US Government entities to complete the RMF process. Many do not know where to begin and there is little to no support up the chain to assist those who are charged with making it happen. The training is beneficial to a point, however difficult when it must be generic and cannot be conducted for individuals with like projects at the same time to allow for specific examples that would apply to the entire group.

27. RMF is a good baseline, but there is so much more to securing our DoD systems. I disagree that RMF alone is an effective solution for DoD systems.

28. I have not been able to utilize tailoring as of yet and that was an intriguing concept I learned about in RMF training. I think the transformation from DIACAP to RMF would have been much tougher without training due to the vast differences.

29. RMF is too cumbersome of a process to be relevant. When it takes months to perform a process (and the interim is a "waiver" for completing prior to deadline/expiration) the whole process is questioned as being needed at all.

30. Formal training is important to fully implement the RMF process. RMF requires the involvement of a much larger group of people with broader areas of responsibility. Organizational commitment to the process and to the use of the resources required is critical

31. The Army culture is making RMF implementation very difficult. Until day to day cybersecurity is prioritized at the lowest echelons, RMF benefits will not be realized.

32. For RMF to be sustainable for the government the Cybersecurity workforce would need to be doubled as well as clear continuous monitoring guidance published.

33. The effectiveness, sustainability or commitment is all more related to how leadership deals with the results than how I feel about it. We are still in DIACAP.

34. The RMF is very system oriented and tough to implement effectively at Federal agencies. Programs like ISO 27001/27002 which are more Tier 1 oriented seem to be more streamlined and less cumbersome for an organization to implement.

35. Once fully enacted by the organization, RMF can support the organizational needs for effectiveness, regardless of training by the practitioner.

36. I have delivered RMF training to numerous government agencies, private companies and military organizations. What I consistently see is a lack of resources and a failure of leadership to appreciate the level of effort because they have themselves failed to take the time to understand what is required. I have seen several instances where no one has even begun performing the necessary steps for their programs. Systems are running without ATO's despite passing many deadlines. I feel that their needs to be a prioritization of systems and a reallocation of resources to even begin making progress in this area. As an aside image the resource constraints once the private sector needs to implement the RMF as part of the critical infrastructure program.

37. RMF is a competent process, however it is not adequately trained or understood by those who perform it. Too often the simple explanation is lost in a library of NIST SP 800 Series, which once read is not synthesized to a usable reference for day to day application. The concepts are fine for discussion, but the measure required to assess and validate a system is often misunderstood or too labor intensive for the average ISSM/ISSO and the ISSE. Lack of DT&E and OT&E background and time and qualified personnel for routine Configuration Management is an Achilles Heel, which is the single fundamental that must be accurately executed first in order to have any baseline security.

38. RMF is a great idea, the concepts are general security best practice, but for DoD and government, each department, component, or entity tends to interpret the NIST instruction differently. And when you come across non-enterprise or non-traditional computer systems, many with specific functions and mixes of technologies, everyone has their own interpretation of what applies and how best to secure these systems. Also, in my personal experience, too much emphasis is placed upon the administrative side, focusing on paperwork, policies, data entry, and following the business process rules for whichever entity you are supporting, rather than focusing on actually securing the system. Its more planning than execution. Personally, I believe in the idea of RMF, but from what I've seen and worked with, the execution of the framework is the problem.

39. RMF training is a Cyber Security necessity.

40. Viability of the RMF process to a great extent depends on Tier 1 Participation, Education and Commitment.

41. My biggest hesitation with the RMF process is the commitment and knowledge that senior management with the process. Most senior managers with whom I've

dealt have very little knowledge of the process and still try to treat it as they did DIACAP.

42. As with any training, I feel that only hands-on and OJT are the best.

Appendix F

Frequency Analysis Tables

RMF Effectiveness

Effective 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2.00	2	2.5	2.5	2.5
	3.00	6	7.4	7.4	9.9
	4.00	4	4.9	4.9	14.8
	5.00	18	22.2	22.2	37.0
	6.00	24	29.6	29.6	66.7
	7.00	27	33.3	33.3	100.0
	Total	81	100.0	100.0	

Effective 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	1	1.2	1.2	1.2
	2.00	2	2.5	2.5	3.7
	3.00	4	4.9	4.9	8.6
	4.00	6	7.4	7.4	16.0
	5.00	15	18.5	18.5	34.6
	6.00	22	27.2	27.2	61.7
	7.00	31	38.3	38.3	100.0

	Total	81	100.0	100.0	

Effective 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2.00	3	3.7	3.7	3.7
	3.00	1	1.2	1.2	4.9
	4.00	11	13.6	13.6	18.5
	5.00	9	11.1	11.1	29.6
	6.00	23	28.4	28.4	58.0
	7.00	34	42.0	42.0	100.0
	Total	81	100.0	100.0	

Effective 4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2.00	3	3.7	3.7	3.7
	3.00	3	3.7	3.7	7.4
	4.00	6	7.4	7.4	14.8
	5.00	13	16.0	16.0	30.9
	6.00	27	33.3	33.3	64.2
	7.00	29	35.8	35.8	100.0
	Total	81	100.0	100.0	

RMF Commitment

Commitment 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2.00	1	1.2	1.3	1.3
	3.00	3	3.7	3.8	5.0
	4.00	5	6.2	6.3	11.3
	5.00	15	18.5	18.8	30.0
	6.00	22	27.2	27.5	57.5
	7.00	34	42.0	42.5	100.0
	Total	80	98.8	100.0	
Missing	System	1	1.2		
Total		81	100.0		

Commitment 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2.00	1	1.2	1.3	1.3
	3.00	3	3.7	3.8	5.1
	4.00	5	6.2	6.3	11.4
	5.00	14	17.3	17.7	29.1

	6.00	21	25.9	26.6	55.7
	7.00	35	43.2	44.3	100.0
	Total	79	97.5	100.0	
Missing	System	2	2.5		
Total		81	100.0		

Commitment 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	1	1.2	1.3	1.3
	2.00	3	3.7	3.8	5.1
	3.00	2	2.5	2.5	7.6
	4.00	6	7.4	7.6	15.2
	5.00	10	12.3	12.7	27.8
	6.00	26	32.1	32.9	60.8
	7.00	31	38.3	39.2	100.0
	Total	79	97.5	100.0	
Missing	System	2	2.5		
Total		81	100.0		

Commitment 4

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	1.00	1	1.2	1.3	1.3
	2.00	3	3.7	3.8	5.0
	3.00	3	3.7	3.8	8.8
	4.00	6	7.4	7.5	16.3
	5.00	12	14.8	15.0	31.3
	6.00	24	29.6	30.0	61.3
	7.00	31	38.3	38.8	100.0
	Total	80	98.8	100.0	
Missing	System	1	1.2		
Total		81	100.0		

RMF Sustainability

Sustainability 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	3	3.7	3.7	3.7
	2.00	5	6.2	6.2	9.9
	3.00	6	7.4	7.4	17.3
	4.00	9	11.1	11.1	28.4
	5.00	21	25.9	25.9	54.3
	6.00	15	18.5	18.5	72.8
	7.00	22	27.2	27.2	100.0

	Total	81	100.0	100.0	

Sustainability 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	3	3.7	3.7	3.7
	2.00	7	8.6	8.6	12.3
	3.00	5	6.2	6.2	18.5
	4.00	7	8.6	8.6	27.2
	5.00	25	30.9	30.9	58.0
	6.00	14	17.3	17.3	75.3
	7.00	20	24.7	24.7	100.0
	Total	81	100.0	100.0	

Sustainability 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	3	3.7	3.8	3.8
	2.00	7	8.6	8.8	12.5
	3.00	2	2.5	2.5	15.0
	4.00	8	9.9	10.0	25.0
	5.00	22	27.2	27.5	52.5

	6.00	16	19.8	20.0	72.5
	7.00	22	27.2	27.5	100.0
	Total	80	98.8	100.0	
Missing	System	1	1.2		
Total		81	100.0		

Sustainability_4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	3	3.7	3.7	3.7
	2.00	5	6.2	6.2	9.9
	3.00	6	7.4	7.4	17.3
	4.00	15	18.5	18.5	35.8
	5.00	19	23.5	23.5	59.3
	6.00	12	14.8	14.8	74.1
	7.00	21	25.9	25.9	100.0
	Total	81	100.0	100.0	

Training Hours

Training hours

Training Hours		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	14	17.3	17.3	17.3
	10.00	1	1.2	1.2	18.5
	24.00	1	1.2	1.2	19.8
	32.00	23	28.4	28.4	48.1
	40.00	16	19.8	19.8	67.9
	46.00	1	1.2	1.2	69.1
	48.00	3	3.7	3.7	72.8
	50.00	2	2.5	2.5	75.3
	56.00	1	1.2	1.2	76.5
	64.00	1	1.2	1.2	77.8
	70.00	1	1.2	1.2	79.0
	80.00	3	3.7	3.7	82.7
	100.00	11	13.6	13.6	96.3
	120.00	1	1.2	1.2	97.5
	160.00	1	1.2	1.2	98.8
	35040.00	1	1.2	1.2	100.0
	Total	81	100.0	100.0	

Appendix G

IRB Approval Letter

IRB Approval Letter

July 11, 2018

Phillip Schall

PSchall5713@ucumberlands.edu

RE: Risk Management Framework

During the week of July 9, 2018, your IRB was approved.

Approval Type & Approval Number	Expedited	0196
Principal investigation	Phillip Schall	
Expiration Date Study	July 11, 2019	
Faculty Advisor	Dr. Oni Oludotun	
Consent Form	Included	
Advertising & Recruitment Materials	Included	
Other Study Documents	Community Partner Letter, Data Collection Tools	
Total Number of Subjects Approved	100	
Changes Needed for Approval	None	

Principal investigators are responsible for ensuring that studies are conducted according to the protocol. As a principal investigator, you have multiple responsibilities to the IRB, the research subjects and the faculty advisor. If you have questions about them, please feel free to call or email Christopher.leskiw@ucumberlands.edu

Christopher Leskiw, Ph.D.
Professor of Political Science
Associate Dean of Academic Affairs
University of the Cumberlands
7557 College Station Drive
Williamsburg, KY 40769

There are five conditions attached to all approval letters:

1. No subjects may be involved in any study procedure prior to the IRB approval date or after the expiration date. (PI's are responsible for initiating Continuing Review proceedings. See the IRB website on the MyUC site or call us for more details.)
2. All unanticipated or serious adverse events must be reported to the IRB within 5 days.
3. All protocol modifications must be IRB approved prior to implementation unless they are intended to reduce risk. This includes any change of investigator or site address.
4. All protocol deviations must be reported to the IRB within 5 days.
5. All recruitment material and methods must be approved by the IRB prior to being used.