ABSTRACT

Title of Dissertation: SELECTING CYBERSECURITY RISK IDENTIFICATION AND ASSESSMENT APPROACHES FOR CRITICAL INFRASTRUCTURE

Shawn Paul Janzen,
Doctor of Philosophy, 2025

Dissertation directed by: Dr. Wayne Lutters, Professor,
College of Information Studies

Critical infrastructure is essential for the successful functioning of societies, while cybersecurity ensures its resilience. To this end, risk identification and continuous assessment are crucial. Managers employ various methods, models, frameworks, standards, guidance, tools, and procedures for these tasks. Hundreds of these approaches for cybersecurity risk identification and assessment exist, differing widely in scope, design, requirements, and implementation. Previous research has reviewed these approaches, examined the contexts in which they operate, and provided guidance on their selection. However, despite the pressing need to secure critical infrastructure and previous work in the field, little is known about which CSRI&A approaches cybersecurity managers use or the reasons behind their choices. My findings indicate that while NIST and ISO-related approaches are common

choices, most managers utilize multiple methods, often pairing NIST or ISO approaches with specialized options, such as NERC CIP, or more flexible ones like CIS 18. Custom approaches are also prevalent.

This study is a two-stage mixed-methods design consisting of 22 semi-structured interviews that informed a survey of 216 participants. All were cybersecurity managers, ranging from middle management to C-suite executives, representing all 16 of the US CISA-designated critical infrastructure sectors. Using a novel conceptual framework that synthesizes theories from technology adoption, decision-making, and information behavior, I assessed whether managers selected their approaches based on fundamental, functional, or situational differences. Results demonstrated the framework's utility, particularly in capturing the multidimensional nature of approach selection through construct unions. Situational context emerged as a consistent modifier in most decision-making processes.

Three additional themes regarding approach selection emerged from the analysis. First, consultants play a pivotal role in the development, selection, and often implementation of these approaches. Second, there is a disconnect between the types of risk measurement preferences that managers express as ideal and what they actually use. Third, the compatibility between approaches matters, given that most managers employ more than one approach. These three themes also drive the need for creating custom solutions.

To triangulate these findings and address the complexity of multivariate data, I developed a method using association rules to construct thematic profiles based on managerial and organizational traits that co-occur with each approach use. Analyzing

the 23 main approaches identified in the study, managers revealed distinct selection differences based on managerial level, involvement of internal or third-party accounting and finance teams, cyber insurance requirements, and individual perspectives on issues such as price value and the absence of effective approaches for operational technologies.

By enhancing understanding of approach selection, I aim to improve management decision-making strategies, raise awareness for approach development, and strengthen cybersecurity risk information-sharing programs. This advances the field by focusing on high-level managers as individual decision-makers whose choices influence both their own work and broader cybersecurity practices within their organizations, thereby bridging the gap between individual agency and organizational outcomes. By empirically examining the actions and perspectives of these individuals, my study provides new insights into how managerial discretion and context interact to shape risk management strategies at the organizational level. My practical aim is to offer innovative profile-based support to managers to improve their approach selection process. This will also inform developers of new approaches and the consultants who recommend them.

SELECTING CYBERSECURITY RISK IDENTIFICATION AND ASSESSMENT APPROACHES FOR CRITICAL INFRASTRUCTURE

by

Shawn Paul Janzen

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2025

Advisory Committee:
Dr. Wayne Lutters, Chair
Dr. Lawrence Gordon
Dr. Charles Harry
Dr. Martin Loeb
Dr. Susan Winter

Dedication

To my wife, Paige, who has been my champion and best friend these many years making everything possible.

To my parents, without whom I would not be here, for giving me an early appreciation for education, who taught me to ask way too many critical questions, and who thought it was a great idea that I do this thing called college and become the first in my family with a degree.

To my chair Wayne L., whose boundless patience and overly generous time never gave up on me and guided me to this moment.

To my friends and other family members, whose many celebrations and daily ongoings I missed while doing this thing called research.

Acknowledgements

To Susan W., the first person I met at the iSchool and asked me about teaching stats for a growing information science program that helped kickstart this journey.

To Charlie H., with whom I greatly enjoyed talking about network graphs and has been reviewing my work since my integrated paper.

To Marty L. & Larry G., the first Smith faculty members I got to know after knocking on Marty's door seeking someone at Smith that worked on cyber risk issues and surprised to find Marty ready to go with flyer with his top publications with Larry.

To Jessica D., the Hail Mary editor with flair.

To Pramod C., Jonathan B., Myeong L., Eric N., Lori P., and TJ R., for our many nerdy conversations, brainstorming, and keeping each other accountable; we walked it together and alone at the same time.

To Jason F., who said yes enough to help overcome all those that said no.

To the Kogod leadership, my fellow faculty, and TAs who provided extra support during this final push.

Table of Contents

Dedication ii
Acknowledgements iii
Table of Contents iv
List of Tables vi
List of Figures viii
List of Abbreviations ix
Chapter 1: Introduction 1
1.1 Challenges of Critical Infrastructure and Cybersecurity 1
1.2 The Wild West of Cybersecurity Risk Identification and Assessment Approaches 5
1.2.1 Example Approaches for CSR Identification and Assessment 6
1.3 Research Motivation, Purpose, and Questions 8
1.4 Research Design 10
1.5 Contributions 11
1.6 Dissertation Structure 11
Chapter 2: Related Literature 13
2.1 Building Toward Analysis of Selecting Cybersecurity Risk Identification and Assessment Approaches 13
2.2 Visualizing the CSR Management Space 15
2.3 Intra- / Interorganizational (Re)Action by Actors 16
2.4 Drivers of Change in CSR Management 18
2.5 Organizational Challenges 20
2.6 Spanning the Gap 23
Chapter 3: Conceptual Framework 28
3.1 Theoretical Foundations for the Conceptual Framework 28
3.2 Mapping Key Theories to the CSR Management Space 33
3.3 Establishing the Conceptual Framework 36
3.3.1 Fundamental understanding differences 39
3.1.2 Functional differences 42
3.1.3 Situational differences 44
3.4 Applying the Conceptual Framework 47
Chapter 4: Study Design 50
4.1 Interviews of Cybersecurity Managers 51
4.1.1 Sampling and Recruitment 52
4.1.2 Interview Data Collection 54
4.1.3 Interview Analysis 56
4.1.4 Interview Limitations 59
4.2 Survey of Cybersecurity Managers 61
4.2.1 Sampling and Recruitment 63
4.2.2 Survey Data Collection 63
4.2.3 Survey Data Cleaning 69
4.2.4 Survey Analysis 71
4.2.5 Survey Limitations 74
4.3 Positional Statement 75
Chapter 5: Findings and Discussion 76

5.1 Study Participants 76
5.1.1 Individual Measures 77
5.1.2 Organizational measures 89
5.2 Addressing RQ1: What CSRI&A Approaches 98
5.2.1 Approaches from Interviews 98
5.2.2 Approaches from Surveys 101
5.3 Addressing RQ2: Why Those CSRI&A Approaches 105
5.3.1 Framework Analysis of Approach Selection 105
5.3.2 Role of External Consultants 124
5.3.3 Qualitative and Quantitative Preferences and Why It Matters 134
5.3.4 Compatible or Conflicting Approaches: NIST versus ISO 151
5.3.5 Association Rules for Approach Selection based on Managerial and Organizational Traits 160
Chapter 6: Conclusion 190
6.1. Summary of Research Study 190
6.2. Summary of Major Findings 192
6.3. Contributions and Implications 194
6.3.1 Scholarly Contributions 194
6.3.2 Practical Implications 202
6.4. Limitations of the Study 204
6.5. Directions for Future Research 206
6.6. Closing Reflection 209
Appendix A. Interview Questions 211
Appendix B. Survey Question Construction 215
B.1 Surveys in Qualtrics 218
B.2 Consent Survey in Qualtrics 218
B.3 Regular Survey in Qualtrics 221
Appendix C. Mapping the Interview to the Research Questions 234
Appendix D: Mapping Survey Battery Question from the Literature and Preliminary Interview Data 236
Appendix E. IRB Approvals 251
Appendix F: Full Size Charts from Chapter 5 259
Glossary 267
Bibliography 271

List of Tables

Table 1 *Select CSR Management Approaches that Include Identification and Assessment* 7
Table 2 *Summary of Management Space Themes Relevant to the Literature* 27
Table 3 *Theories Informing the Conceptual Framework* 29
Table 4 *Conceptual Framework* 37
Table 5 *Mapping Theories of Technology Adoption to the Conceptual Framework* 37
Table 6 *Aspects of the Conceptual Framework* 47
Table 7 *Study Design Elements* 51
Table 8 *Interview Sampling Frame*[1] 53
Table 9 *Changes to Interview Questions* 57
Table 10 *ISAC Outreach* 65
Table 11 *Manager Level by Years of Experience* 78
Table 12 *Number of Managers with CSRI&A Duties by Frequency of Those Duties* 79
Table 13 *Interview Participant Highest Degree* 80
Table 14 *Interview Participant Higher Education by Major* 81
Table 15 *Survey Participant Higher Education by Major and Highest Degree* 82
Table 16 *Certifications per Manger for Risk Management and/or Cybersecurity* 82
Table 17 *Manager Certifications: Risk Management and/or Cybersecurity (Most Frequent)**. 84
Table 18 *Number of Active and Relevant Organizations Per Participant* 85
Table 19 *Top 6 Active and Relevant Organizations* 86
Table 20 *Active and Relevant ISAC Organizations* 87
Table 21 *Manager's Race and Ethnicity* 88
Table 22 *Manager's Gender* 89
Table 23 *Survey and Interview Participant Organization Critical Infrastructure Sector and Subsectors* 91
Table 24 *Organization Type by Size based on Number of Employees - Survey Participants* 93
Table 25 *Organization Type by Size based on Number of Employees - Interview Participants*. 94
Table 26 *ISAC Memberships per Organization* 95
Table 27 *ISAC Memberships* 96
Table 28 *Groups within Organization with CSRI&A as Primary Duties* 97
Table 29 *Number of Groups within Organization Sharing CSRI&A as Primary Duties* 97
Table 30 *Number of Approaches Mentioned in Interviews* 100
Table 31 *Top 7 Selected Approaches by Survey Respondents* 102
Table 32 *Survey Participant CSRI&A Approach Selections and Current Use Status* 103
Table 33 *Approach Measurement Preferences by Managerial Level* 137
Table 34 *Comparing ISO and NIST Approaches Selected by Survey Participants* 154
Table 35 *FAIR Approach Top Eight Rules Sorted by Lift* 164
Table 36 *Traits and Lift by Approach* 166
Table 37 *Association Rules Traits - Approaches by Level of Management* 182
Table 38 *Association Rules Traits - Approaches by Accounting and Finance Teams* 184
Table 39 *Approaches by Select Custom Approach Profile Traits* 185
Table 40 *Example Survey Question Development from the Literature** 215
Table 41 *Mapping the Conceptual Framework to Interview and Research Questions* 234

Table 42 *Mapping Survey Battery Questions from the Literature and Preliminary Interview Data* 236
Table 43 *Manger Certifications: Risk Management and/or Cybersecurity* 259
Table 44 *Heatmap Table of Approaches and Traits (Full)* 261

List of Figures

Figure 1 *My mindmap of CSR identification and assessment approach selection* 4
Figure 2 *My Mindmap of Challenges to CSRI&A Approach Selection within the CSR Management Space* 16
Figure 3 *Key Theories Toward CSRI&A Approach Selection within the CSR Management Space* 34
Figure 4 *Study Design Flow* 50
Figure 5 *Percent of Managers with CSRI&A Duties by Frequency of Those Duties* 79
Figure 6 *Frequency Variance from Mean of Participants per Critical Infrastructure Sector* ... 92
Figure 7 *Frequency of Selected Approaches by Survey Respondents** 103
Figure 8 *Conceptual Framework with Overlapping Constructs* 114
Figure 9 *Current and Potential Future Conceptual Framework Designs* 123
Figure 10 *Potential Future Conceptual Framework with Multi-Construct Design* 123
Figure 11 *Measurement Preference Percentage* 137
Figure 12 *Stacked Count Measurement Preference by Organization Sector* 139
Figure 13 *Typical Risk Management Heat Map* 145
Figure 14 *Tapestry, a Web-based Application for Risk Assessment* 146
Figure 15 *Survey Participant Counts of ISO and NIST Approach Current Use Status* 154
Figure 16 *FAIR Approach Profile - Most Frequent Traits from Top 100 Association Rules by Lift* 167
Figure 17 *FAIR Approach and Top Traits by Frequency as Bipartite Ego Graph Network* 168
Figure 18 *NIST SP 800-30 Approach Profile - Most Freq Traits from Top 100 Association Rules by Lift* 171
Figure 19 *NIST SP 800-30 Approach and Top Traits by Frequency as Bipartite Ego Graph Network* 172
Figure 20 *NIST SP 800-37 Approach Profile - Most Freq Traits from Top 100 Association Rules by Lift* 174
Figure 21 *NIST SP 800-37 RMF Approach and Top Traits by Frequency as Bipartite Ego Graph Network* 175
Figure 22 *ISO 27005 Approach Profile - Most Frequent Traits from Top 100 Association Rules by Lift* 177
Figure 23 *ISO 27005 Approach and Top Traits by Frequency as Bipartite Ego Graph Network* 178
Figure 24 *Custom / Bespoke approach (developed in-house and/or with third-party help)* 179
Figure 25 *Custom / Bespoke Approach and Top Traits by Frequency as Bipartite Ego Graph Network* 180
Figure 26: *A Simplified Risk Management Cycle for Cybersecurity* 269

List of Abbreviations

ACC	American Chemistry Council
AEHIS	Association for Executives in Healthcare Information Security
CompTIA	Computing Technology Industry Association
CERT	Computer Emergency Readiness Team
CDPSE	Certified Data Privacy Solutions Engineer
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CGEIT	Certified in Governance of Enterprise Information Technology
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISA	Critical Infrastructure and Security Agency
CISM	Certified Information Systems Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CPS	Cyber-physical system
CRISC	Certified in Risk and Information Systems Control
CRS	Congressional Research Service
CSF	Cybersecurity Framework
CSR	Cybersecurity risk
CSRI&A	Cybersecurity risk identification and assessment
CSN	Cybercrime Support Network
DHS	Department of Homeland Security

DIB	Defense Industrial Base
DIT	Diffusion of innovation theory
DoD	Department of Defense
DNG	Downstream Natural Gas
DTT	Disruptive technology theory
EC-Council	International Council of E-Commerce Consultants
ENISA	European Union Agency for Cybersecurity
EI	Elections Infrastructure
EO	Executive order
ERP	Enterprise Resource Planning
FAIR	Factor Analysis of Information Risk
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FS	Financial Services
GDPR	General Data Protection Regulation
GSEC	Global Information Assurance Certification
H (H-ISAC)	Health (Health Information Sharing and Analysis Center)
HIPPA	Health Insurance Portability and Accountability Act
I&A	Identification and assessment
IAASB	International Auditing and Assurance Standards Board
IEC	International Electrotechnical Commission
ICMA	International City/County Management Association
IER	Insufficient Effort Responding

IG	Implementation Groups
IRB	Institutional Review Board
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association (deprecated; goes by ISACA)
ISSA	Information Systems Security Association
ISC	International Information System Security Certification Consortium
IT	Information technology
ME	Media + Entertainment
MS	Multi-State
MTS	Maritime Transportation Services
NACD	National Association of Corporate Directors
NASA	National Aeronautics and Space Administration
NASCIO	National Association of State Chief Information Officers
ND	National Defense
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
OCTAVE	Operationally Critical Threat and Vulnerability Evaluation
ONE	Oil & Natural Energy
ONG	Oil & Natural Gas
OT	Operational technology

PHA	Process Hazards Analysis
PMP	Project Management Professional
PT & ORTB	Public Transportation and Over-the-Road Bus
PwC	Pricewaterhouse Cooper
RCT	Rationale choice theory
RE	Real Estate
REN	Research Education Networks
RH	Retail and Hospitality
RI&A	Risk identification and assessment
RIMS	Risk Management Society
ROI	Return on Investment
RMF	Risk Management Framework
RQ	Research question
SAE	Society of Automotive Engineers
SANS	SysAdmin, Audit, Network, Security (for the SANS Institute)
SSCP	Systems Security Certified Practitioner
S&T	Science and technology
TAM	Technology adoption model
US	United States

Chapter 1: Introduction

The increasing frequency and impact of cyber threats facing critical infrastructure underscore the urgent need for effective cybersecurity risk identification and assessment (CSRI&A). This dissertation investigates not only what approaches managers choose, but also why these choices emerge in the complex context of modern organizations. By analyzing the decision-making processes of cybersecurity risk (CSR) managers, this study seeks to illuminate both the practical challenges and broader implications—offering insights that address immediate operational concerns while informing policy and organizational strategy. The following chapter opens by detailing the prevailing challenges shaping this critical domain.

1.1 Challenges of Critical Infrastructure and Cybersecurity

Critical infrastructure are the assets essential to the economy, public health, national security, encompassing both physical and virtual systems. Any disruption to that infrastructure can generate debilitating and cascading effects throughout industry, government, and society. For example, the Federal Bureau of Investigation's 2024 Annual Internet Crime Report documented 4,878 incidents against US critical infrastructure associated with $1.571 billion in losses (US FBI, 2024, p. 12), demonstrating the persistent threat from criminal cyber actors. The Colonial Pipeline ransomware attack in the spring of 2021, impacted nearly half of the US East Coast's oil-derived fuel supply (Shier, 2021), exemplifies the potential consequences of successful external breaches. Meanwhile, Verizon's 2025 Data Breach Investigations Report shows that nearly one-third of breaches involve third parties, highlighting how vendor relationships and supply chain exposures expand the attack surface and introduce new forms of risk (2025, p. 5). Together, these cases demonstrate that modern cyber risks are both multifaceted and

interconnected, requiring critical infrastructure organizations to adopt comprehensive risk identification and assessment strategies responsive to a constantly shifting threat landscape.

Cybersecurity management is not only a necessary and important organizational function protecting against external cyberattacks, it also considers internal threats when adopting new technologies such as cloud services (Nicholson, 2018) and ensures that security adjustments meet new regulatory compliance requirements like the European Union's General Data Protection Regulation (GDPR) (Li et al., 2019). Each level of the US Government carries the burden and challenge of cybersecurity responsibility for its own information and operational systems. In addition, this management represents the government's shared responsibility in the cybersecurity of critical infrastructure—infrastructure which is almost wholly managed by private organizations (White House, 2013).

A key facet of strong cybersecurity is good risk management, which requires good risk identification approaches. I use the term approach to represent the wide range of decision support aids used to understand risk identification and assessment (I&A), such as methods, models, frameworks, guidance, tools, and procedures. When risks are wrongly identified, or not identified at all, the rest of the process is potentially biased and vulnerable to severe threats. The National Electric Sector Cybersecurity Organization Resource (NESCOR) had detailed risk failure scenarios with impacts such as "loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence" (Christopher & Lee, 2013). For this reason, both risk identification and assessment should be the highest priority for risk management (Hubbard & Seiersen, 2016). The value of risk management is hard to quantify except in the absence of loss. Once implemented, alternatives cannot also be implemented and compared. Thus, responsibility for the cybersecurity of critical infrastructure, which supports

vast, complex parts of the US economy, health, and other vital systems, means that cybersecurity risk managers need to choose their risk I&A approaches well. This dissertation will offer insights into risk I&A approach selection and provide advice to cybersecurity risk managers.

The first pillars in the 2018 US National Cyber Strategy includes, "Manage cybersecurity risk to increase the security and resilience of the Nation's information and information systems." (White House, 2018, p. 6). Thus, the US government's highest executive office identified risk management as integral to the practice of cybersecurity, placing heavy emphasis on the importance of accurate cyber risk I&A. Cybersecurity has the same inherent core functions and overarching principles as physical security with respect to risk management.

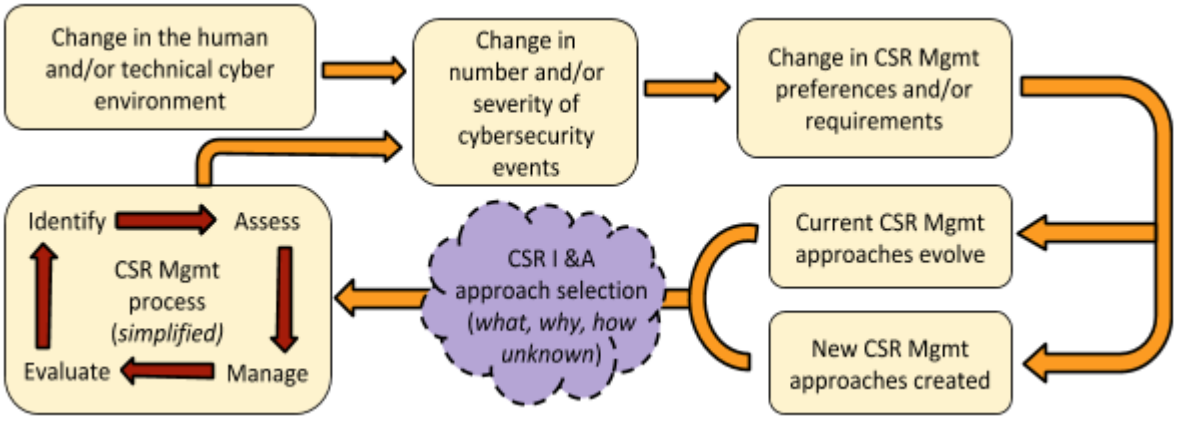
CSRI&A is inherently multi-layered. At the macro level, shifts in national security priorities, regulatory requirements, and the broader threat landscape shape the environment in which organizations must operate. However, organizations, at a meso level, each interpret and incorporate these external drivers according to their own resources, missions, and structures. The micro level—represented by individual CSR managers—reflects the point of action where these pressures are interpreted, negotiated, and ultimately enacted in concrete risk management choices. These levels are interdependent: macro policies cascade down to organizations, which then provide both constraints and leeway for managerial decision-making. Yet, feedback flows upward too, as patterns of individual and organizational behavior collectively influence regulatory expectations and market standards.

I observed that cyber risk management does not occur in isolation, but instead exists within a specific CSR management space and context. Cyber risk management is part of a greater system, and aspects of that system may have directly and indirectly influenced the

approaches used to conduct CSRI&A within the CSR management processes, reflected in Figure 1.

Figure 1

My mindmap of CSR identification and assessment approach selection



The CSR management space displayed in Figure 1 can be understood as the dynamic zone where macro, meso, and micro factors intersect. The macro context (e.g., federal mandates, global threat intelligence) defines boundary conditions for all organizations, but each organization filters and operationalizes these according to specific industry requirements, available resources, and internal culture at the meso level. Within this organizational setting, individual managers (micro level) interpret, balance, and sometimes challenge organizational directives based on their professional judgment, experience, or access to information. The interplay within this management space thus involves negotiation—between the collective needs and risk postures of the organization and the discretionary judgments of individual managers—shaped by overarching external drivers.

1.2 The Wild West of Cybersecurity Risk Identification and Assessment Approaches

The US Wild West was a decentralized, expansive frontier region for white settlers; a time characterized by inventiveness, territoriality, and self-reliance. Today's modern marketplace of CSR approaches shares these attributes: individuals and organizations served as creators and vendor agents to supply diverse approaches through this distributed network marketplace to meet public and private CSR managerial needs as they evolve in response to shifting dynamics of the cybersecurity landscape (Congressional Research Service, 2019, p. 16).

To demonstrate a portion of this decentralized, expansive landscape and a starting point for possible solutions, the software marketplace Capterra recently listed 107 different IT risk management approaches, mostly software tools, from different vendors (Capterra, 2020). In 2006, the European Union Agency for Cybersecurity (ENISA) detailed a risk assessment inventory consisting of 17 methods and 28 tools from 14 and 25 organizations around the world respectively, which ENISA called a non-exhaustive, open list chosen by popularity (ENISA, n.d.; see also Panagiotis et al., 2013). Some of the ENISA inventory items appeared as both methods and tools based on vendor description, further supporting how terminology for approaches are not consistent.

Despite this variety, the 2016 US Federal Cybersecurity Research and Development Strategic Plan recommended development of new approaches, as the authors found the risk management domain a "relatively mature field," yet that CSR management remained challenged by uncertainties, inaccuracies and affected by complex governance systems (National Science and Technology Council, 2016, p. 30-31). With a wide range of CSR management approaches from which to choose and that vary as to their inclusion of I&A aspects, options to mix-and-

match existing approaches, and reports calling for even more approaches, it is important to grasp that this large, dynamic marketplace may affect elements of approach selection.

If CSR managers have some discretion in choosing their approaches, they may select different approaches to use in their CSRI&A process as part of the risk management cycle. The approach is meant to serve the CSR manager as a decision-support aid toward identifying and assessing cybersecurity risks, and so the selection of the approach and resulting I&A of the cybersecurity risk are different activities. What is unclear from the literature, and thus my primary contribution, is to understand what, why, and how CSR managers select their approaches for CSRI&A.

1.2.1 Example Approaches for CSR Identification and Assessment

To facilitate a discussion of selecting approaches for CSRI&A, it is helpful to provide examples that could be selected, even though individual approaches are not needed to establish the conceptual framework in Chapter 3. For this subsection, I discuss three risk management approaches which included risk I&A, listed in Table 1 below, organized by year created. I list the approaches' originations and whether the approach predominately or entirely uses qualitative or quantitative methodologies. I selected these three because they represented development from public, private, and academic settings, were all information security specific, and were among the most mentioned approaches across the cybersecurity and risk management literature and professional community spaces that I encountered.

Table 1

Select CSR Management Approaches that Include Identification and Assessment

Tool	Created	Updated	Methodology	Focus	Origin
OCTAVE	1999	2005	Qualitative	Info Sec.	University & US DoD
FAIR	2005	2014	Quantitative	Info Sec.	Private sector
NIST RMF	2010	2018	Qualitative	Info Sec.	US civilian federal government

Operationally Critical Threat and Vulnerability Evaluation (OCTAVE), is a qualitative risk management approach widely adopted across the government and private sector (Alberts & Dorofee, 2002). OCTAVE addresses technical, physical, and human dimensions across an entire organization's information security components. It is a framework for small teams to implement themselves and leverage their expert knowledge. Caralli et al. (2007) described OCTAVE as a complete risk management method with separate steps for identifying and analyzing risk, as well as interdisciplinary analysis across the organization, rooted in technical details and finalizing with a strategic plan. Criticism of this approach is tied to its sizable complexity without the rigor of modeling, high cost for training, and design for large organizations (Bigueur, 2015; Ionita, 2013; Ratcliffe, 2020).

The Factor Analysis of Information Risk (FAIR) approach has a highly detailed, complex taxonomy, and purely quantitative risk assessment approach that is good for risk scenarios. FAIR is concerned less with the source of information assessed and more with the quantified risk potential for data loss by both probability of occurrence and severity of impact. In this regard, FAIR is a complementary approach for use alongside other risk management approaches such as OCTAVE (The Open Group, 2009). While it meets the need for a more quantitative approach

(Freund & Jones, 2014), criticisms include a lack of documentation for use and for its complex implementation procedures (Bigueur, 2015; Ionita, 2013; Ratcliffe, 2020).

The Federal Information Security Management Act (FISMA), part of the US E-Government Act (Public Law 107-347) (US Congress, 2002), directed the US National Institute of Standards and Technology (NIST) to lead development of a risk management framework (RMF) to reduce information security risk. It also specified that provisions for the framework must be usable by both government agencies and operators of critical infrastructure. The RMF, initially released in 2010, follows a six step and preparation process with an activity at each step that is task-based using the inputs, outputs, roles, and discussions to focus on the categorization and the establishment of risk-related controls (NIST Special Publication 800-37 Rev.1, 2012). The RMF allows for flexible execution so that organizations can still meet other information security and privacy obligations. Criticisms of this approach are that it uses excessive government jargon and cross-referencing to other US policy documents and standards, that it is highly subjective, lacks quantification, requires many users in different roles, and the ambiguity in its design reduces its specificity (Bigueur, 2015; Maclean, 2017).

1.3 Research Motivation, Purpose, and Questions

Cyber breaches of US critical infrastructure, tracked by the FBI and Cybersecurity and Infrastructure Security Agency (CISA), are increasing. Fourteen of the 16 US critical infrastructure sectors had incidents of ransomware and five critical infrastructure sectors were compromised (CISA, 2022; US FBI, 2021). Ransomware, along with data breaches are the most reported cyber threats on critical infrastructure (US FBI, 2024). Despite the importance of protecting critical infrastructure and numerous policy documents on this issue, currently little is

known as to what CSRI&A approaches are used to secure critical infrastructure and why those approaches were selected.

The purpose of my research is to gain a better understanding of this decision-making and adoption activity within a critical infrastructure context and provide guidance on approach selection to cybersecurity managers toward enhancing infrastructure cybersecurity resiliency. My aim is to apply the specific CSR management space discussed here as the use case to address the goal of successful cybersecurity for US critical infrastructure conducted by cybersecurity managers. To accomplish cybersecurity goals for critical infrastructure, strong CSRI&A is necessary and relies upon approaches that work well for each CSR manager and organization. Because the decision-making aspects for the domain of CSR management are underdeveloped, I conducted an exploratory study. The CSR management space establishes the context from which I derive my research questions. There is a vast marketplace of CSRI&A approaches from which to choose, which prompts my first research question (RQ):

1. Which approaches, if any, do cybersecurity managers select for the risk identification and assessment of critical infrastructure? Are there any approaches actively not selected?

Trend analysis becomes possible by knowing which approaches are used, but that is superficial without knowing how and why they were selected. In the next chapter, I extend the discussion to elements that may influence the CSR management space and thus affect which CSRI&A approach was selected, prompting my second research question.

2. What factors affect how and why cybersecurity managers select the approaches they employ for risk identification and assessment of critical infrastructure?

Understanding these decision elements, I can examine the cybersecurity managers' information behaviors and knowledge landscapes (Hakken, 2003), organizational and individual

approach selection fit, and other determinants that will help me develop guidance for cybersecurity practitioners and areas for discussion among cybersecurity and critical infrastructure scholars and policymakers.

The complex interplay between the macro, meso, and micro levels is central to this research. Organizational leaders make policy-level decisions that reflect external (macro) imperatives, yet the translation into effective practice depends critically on the actions and judgments of individual managers (micro). This introduces both opportunities for innovation, as individuals adapt or refine practices to fit unique contexts, and risks, as inconsistent interpretation can lead to gaps or conflicts between strategy and execution. By focusing on how managers select CSRI&A approaches within organizational constraints, this study addresses how macro-level pressures and meso-level processes are mediated at the micro level, and how, in turn, those micro-level decisions may shape organizational and even industry practice.

1.4 Research Design

I conducted this dissertation in two parts to explore CSRI&A approach selection. The first part consisted of semi-structured interviews with high-level cybersecurity manager key informants. The second part surveyed mid-to-high level cybersecurity managers and validated interview findings of approach selection preferences, avenues for learning and engagement, approaches used, and managerial discretion to choose approaches. A novel conceptual framework, scaffolded from theories of technology adoption, decision-making, and information sharing helped generate findings for RQs 1 and 2. Constructs from the conceptual framework provided hooks into the interview and survey data to help explain key patterns of decision behavior and areas of (dis)agreement. Interview and survey data was self-reported and provided user and leadership-based perspectives.

1.5 Contributions

My research will make several contributions to scholarship and practice. This work advances new exploratory analysis into management and policy with respect to decision-making, cybersecurity, risk management, and critical infrastructure. Perhaps most importantly, given the ongoing threat of cyber events, this work may help foster more and new conversations within the CSR management community regarding merits and methods they use to find and select approaches. Additionally, participants' perspectives shared through this work may also contribute to a greater discussion regarding how risk is measured. Altogether, this could lead to adopting approaches that better fit those cybersecurity managers and their organizations and hopefully improve critical infrastructure's overall security positions. From a data collection perspective, this study will yield results from a professional community that is difficult to access. Moreover, the combination of mid-and-upper-level cybersecurity managers are a group not often the subject of academic research. Findings from this sample could help lead to more meaningful engagement between strategic and operational levels of management. Public policy leaders and researchers with this study's insights may further studies in areas such as implementation, feasibility, ambiguity, and diffusion. Managers and management scholars may find it useful for better understanding administrative discretion, resource allocation, and individual and organizational learning. Overall, this work helps advance the CSR management body of knowledge and serves as a study upon which future work may build.

1.6 Dissertation Structure

This section outlines the remainder of this dissertation. Chapter 2: Literature Review contains prior work and other background information which together establishes an outline of the cybersecurity management space necessary to investigate the CSRI&A selection process.

Chapter 3: Conceptual Framework describes the conceptual framework and how I use it to assess participant data. Chapter 4: Study Design explains this proposal's overall study design and methodology, introduced in the section above. Chapter 5: Findings and Discussion reveals findings from interviews and surveys and explores these results. Lastly, Chapter 6: Conclusion summarizes the dissertation, my contributions to scholarship and practice, discusses research limitations, postulates on future work, and closes out the dissertation.

Chapter 2: Related Literature

In this chapter, I discuss the relevant theoretical and practical works, literature, and policies that help provide the foundation and boundaries for this research. I start by setting a high-level overview of factors that may influence how cybersecurity managers may initially consider CSRI&A approaches. Then, I expand to discuss other types of factors in greater detail, such as managerial reaction to external forces, shifts in management preferences, and organizational changes.

2.1 Building Toward Analysis of Selecting Cybersecurity Risk Identification and Assessment Approaches

Based on the literature, I detail three facets to establish the foundation for discussing factors that may affect how a cybersecurity manager selects risk identification and assessment approaches. First, risk I&A is a key aspect of security work, including cybersecurity. It follows that minimizing various aspects of risk improves security. Second, while approaches such as frameworks, models, methods, and software tools help the risk minimization process by serving as human managerial decision-making support aids, individuals may view such decision aids very differently. Third, how people learn about, choose, and use these approaches is largely dependent upon their past and present information environment. I expand on each step below.

The work of cybersecurity professionals involves constant risk with the chance that unauthorized, unwelcome, and improper use or access to systems, people, or data may occur. Although their approaches differ, cybersecurity professionals generally seek to minimize these risks through reducing exposure to vulnerabilities, threats, and consequences (Ganin et al., 2020). Cybersecurity has the same inherent core functions and overarching principles as our long

understanding of physical security with respect to risk management. Risk managers and cybersecurity professionals accomplish this through a proactive combination of having the right staff, policies, procedures, and tools (Mills & Goldsmith, 2014). Yet, security success also includes the degree to which decision-makers emphasize security aspects of risk communication and behaviors is contextual and understood through individual perception (Williams & Noyes, 2007). Therefore, decision-aids can help support in understanding and communicating risks.

To conduct CSRI&A, cybersecurity managers use various approaches to help support decision-making. However, there are many factors that can influence perception of a personal decision support or the suitability of an approach. Trust is an important factor and includes perceptions of the information received, of measurements used to obtain the information, and in the way cybersecurity managers abstract and communicate risk (Nurse et al., 2011). In addition to trust, Pfleeger and Caputo (2012) found other individual characteristics to include cognitive load, bias, and behavioral aspects of security contributed toward awareness, attitude toward, and use of cybersecurity products and processes. While individual preferences and viewpoints affect the choice to use an approach to support decision-making or not, this is all done within the context of the information environment.

Cybersecurity managers evolve professionally and develop their views through numerous avenues. A task-oriented approach suggests that learning occurs by taking actions that fit the environment and reduce uncertainty through task and role assignments (Thompson, 1965). This is reinforced through associative professionalization and bureaucratization (Hall, 1968). Cybersecurity advocates, also called champions, can actively promote the selection of cybersecurity actions and preferences of individuals broadly (Alshaikh, 2020; Haney & Lutters, 2018). Development occurs through communities of practice, extending what is possible through

the cybersecurity manager's home organization alone. Ferwerda et al. (2010) indicated that while technical advisory organizations, like Computer Emergency Response Teams (CERTs), have core duties to include threat monitoring and information exchange, they also serve unofficially as information gathering hubs. The cybersecurity manager's various associated organizations also determine and impart the importance of multilateral or cooperative attention and engagement priorities (ibid). The rest of this chapter expands on this foundation presenting various external factors that may influence CSR decision-making and approach selection.

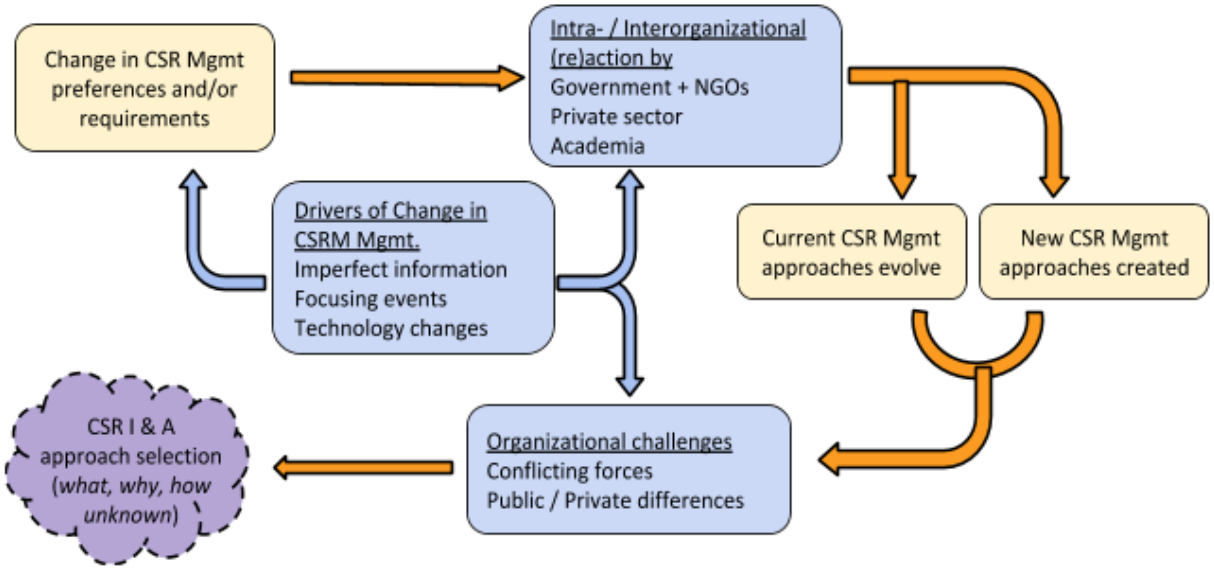
2.2 Visualizing the CSR Management Space

In Section 1.1, I introduced my vision of the CSR management space. Figure 2 serves as a visual reference to organize the related literature on the potential forces and feedback cycles that help inform this space. The interacting elements within this CSR management space directly and indirectly influence the CSRI&A approach selection. Figures 1 and 2 provide a setup for my two research questions, where Figure 1 identifies my contribution to the scholarship in the purple figure element (RQ1), and Figure 2 identifies possible avenues affecting approach selection (RQ2).

Figure 2 juxtaposes elements from Figure 1 with three groups of influential factors, mapping the areas where these forces may occur. The tan elements carry over from Figure 1 while the blue elements describe and represent direction of potential influence. The three groups include intra- and interorganizational (re)actions, drivers of change in CSR management, and organizational challenges.

Figure 2

My Mindmap of Challenges to CSRI&A Approach Selection within the CSR Management Space



In Subsections 2.3 through 2.5, I expand on the three blue groups of Figure 2 with literature connected to topic areas and challenges that may influence selection of CSRI&A approaches in Subsections 2.3 through 2.5.

2.3 Intra- / Interorganizational (Re)Action by Actors

When CSR managers make known that their management preferences and/or requirements are changing, there is an opportunity for agents in the external environment to become involved, either by action or reaction, in the creation of new or evolution of current approaches. Agents within this element come from other parts of the government and nonprofits, academia, and the private sector. One major area of (re)action is in agreement, wherein consensus, support, and resources for CSRI&A approaches can emerge. Where agreement fractures, the landscape of CSRI&A approaches can further diversify and specialize.

At first glance, it may appear there is universal agreement that CSRI&A is important for the protection of critical infrastructure and related systems. However, this agreement ends when it comes to the details of CSRI&A implementation. Agreement from the private sector to use risk management approaches for their vast ownership and operation of US critical infrastructure comes from a mix of economic incentives, including cyber insurance, exchanging best practices, and regulatory pressure (Cherdantseva et al., 2016; Moore, 2010). The agreement resonates through the federal government via recurring policy documents like the US Cybersecurity Strategy (White House, 2018) and ad hoc reports like the Cyberspace Solarium Commission report (2020) that set agreement expectations. However, disagreements in approaches can be seen through omission. While the Solarium report (2020) recommended use of cyber insurance, this approach was absent in the more authoritative US Cybersecurity Strategy (2018) suggesting differences still exist within the federal government. Likewise, the private sector is heterogeneous in its application of economic incentives, with differences existing within groups like banks, hospitals, and electric companies, and the government does not use economic incentives for internal compliance the same way the private sector does (Moore, 2010).

Cross-sector agreement also occurs because government policy for CSRI&A commonly seeks to incorporate private sector best practices (Executive Order 13636, 2013; US Cybersecurity Strategy, 2018). In turn, the US federal government through agencies like NIST also plays a role in the agreement of CSR management between state and local levels of government (Norris et al., 2019). Vendors like IBM and Deloitte produce custom CSR management approaches and offer consulting services to review issues of organizational pressures and task/position legitimacy (Deloitte & NASCIO, 2018; Goel et al., 2018).

Academia and think-tanks also act as boundary agents between sectors, studying, sourcing, and suggesting the CSR management agreement between the private sector and various levels of government. Scholars distill lessons learned from risk I&A of critical infrastructure sectors and advance our agreement of CSR management (Refsdal et al., 2015). Smith and Fischbacher (2009) noted the volume and type of emergent, cascading hazards affect organizational resiliency and cause cybersecurity managers to seek new approach solutions from external agents, such as academic scholars, but those agents may struggle with the multidisciplinary nature of the problems that challenge our previous understanding of risk and resilience.

2.4 Drivers of Change in CSR Management

Drivers of change, which include environmental triggers or internal rethinking and reframing of risk, can impact the organization as well as individual CSR managers and can span across communities of practice. These drivers may influence the development of I&A requirements, preferences, and engagement with other actors in the selection space. The CSR management space is rife with incomplete and incorrect information, which complicates CSR managers' responsibilities to make cyber risk I&A decisions that rely on accurate knowledge about their systems and the situational environment. Focusing events and technology challenges exacerbate this difficulty, impacting downstream change in risk appetite within the CSR management space which can have implications for the selection of CSRI&A approaches.

Focusing events are drastic, severe, interruptive moments that can disrupt cybersecurity management, policy, and professions. They are signals that something went wrong and needs to be treated differently, which prompts changes in the CSR management space. The cyber event hack of a Pennsylvania water treatment plant in October 2006 resulted in new directives that

refined risk standards and response systems (Reddick, 2009). Changes in bureaucratic structures, such as the reorganization of federal agencies and formation of DHS post-9/11, triggered changes in the technological decision-making options available to managers of critical infrastructure and other cyber-physical systems (Moteff, 2005). Executive Order 13800 (2017) made federal agency heads accountable for CSR management within their agencies. This policy is another focusing event whereby agency heads, to meet new accountability standards, may enact greater control over their cybersecurity manager subordinates, which in turn could affect the CSRI&A approach selection.

Contrasting the shock inducements of focusing events, the CSR management paradigm shift comes from the emergence of new structures born from the transference and adaptation of existing systems. The US Department of Defense (DoD) demonstrated this by identification of cyberspace as a new domain of battle; along with it came a formal extension of managing war-related risks recast as cyber risks (Lawson & Middleton, 2019; see also Kello, 2013). Additionally, adaptation of DoD's layered cyber defense as the US national cyber strategy challenged cybersecurity managers to rethink and expand risk concepts that shape behavior, deny benefits, and impose costs (Cyberspace Solarium Commission, 2020). Recognizing the occurrence of a paradigm shift is difficult when experiencing it directly, particularly when the new paradigm shares traits with the previous one.

Rapid advancements in technology can also cause havoc for a CSR manager, especially as human, cyber, physical, and multiplex systems are increasingly interconnected, while deepening their links with critical information systems, infrastructure, and the economy (Agresti, 2010; Sambamurthy & Subramani, 2005; Whitman & Mattord, 2018). Emergent and disruptive technologies reshape the information operations and systems landscape in an organization, thus

inflating the potential for risk. Technologies such as cloud computing and storage (Agresti, 2010; Nicholson, 2018) or the convergence of the Internet of Things (IoT) and cyber physical systems (CPS) (Greer et al., 2019) cause complications with things like user authority, version control, vendor selection, and contingency planning (Whitman & Mattord, 2018). Additional difficulties rise as CSR managers must safeguard information within and between these technologies as organizations collect, use, store, and transfer information at exponentially increasing speeds and scales.

As technologies change, so does the scope of cybersecurity professional needs. The CSR management profession co-evolve their use and adoption of standards and certifications to meet the demands of the transforming economy and technologies, such as the adoption of ISO 31000 risk management principles (Olechowski et al., 2016). However, Hubbard (2009) contended that despite changes to CSR management practices with new risk demands, the broader risk management profession has not evolved its standardized certifications. Such challenges echo in the next subsection.

2.5 Organizational Challenges

Conflicting forces within CSR managers' organizations and professional communities may affect approach selection outcomes. Organizational decision-making has bureaucratic, socio-political, and technical attributes that carry different implications for choosing an approach. Such decisions are often not made in isolation, particularly at higher tiers of cybersecurity management, where issues in security can overlap with those of supply chains, cost and schedule, human capital, organizational and managerial forces, and external dependencies (Gerstein et al., 2016). Such tensions can increase where and when each of these factors enter a manager's span of control (Gulick, 1937; Meier & Bohte, 2000). Even attributes such as

organization size, sector type, and staff availability may cause conflict for selecting CSRI&A approaches that claim to perform better for specific types of organizations. For example, it is a regular challenge within the healthcare industry where cybersecurity managers navigate complex regulatory policies, engage supply chain vendors for medical equipment and electronic records security updates, and lack of resources and support from senior leadership due to leadership's outdated information technology views (Abraham et al., 2019).

Disagreement within the CSR management profession presents a second form of organizational challenge that can affect how approach selections are made. Schisms within cybersecurity communities of practice exist as CSRI&A best practices, reflected in the types of approaches. One of the larger debates pertains to the use of qualitative, quantitative, or mixed methods (Caralli et al., 2007; Hubbard & Seiersen, 2016). One answer is to let the market sort the issue out. However, the CSR management profession has an ongoing reliance on old decision methods, possibly due to treating cybersecurity as sunk costs instead of strategic investments. This is further compounded by an overreliance on CSR decisions supported by anecdotes rather than scientifically grounded analysis (US Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, 2018).

Regardless of efforts to bring the government and private sector closer together on CSRI&A, there is a public/private divide challenging the one-sector-fits-all approaches. It complicates public CSR managerial selections, particularly when instructed to perform more like their private sector counterparts. However, challenging this tension is good. It spans the divide where possible since multi-sector governance of cyber critical infrastructure necessitates cross-sector organizational partnership. While directives toward the government or the public sector

can muddle approach selection and both sectors need to act as if the other is not a monolith, there are some important sector differences that persist.

Among the most prominent organizational challenges between public and the private sector are the divergent organizational environment characteristics cybersecurity managers face and organizational goals they support (Caudle et al., 1991; Rosacker & Olson, 2008). Managers of public information systems contend with greater operational constraints, such as accountability and red tape than do their private sector counterparts (Bretschneider, 1990). The private sector has its fair share of cybersecurity hurdles which affect their bottom lines, including issues with intellectual property and trade secrets, while the public sector's cyber challenges include the provision of public goods. For organizational goals, publicly traded organizations are accountable to their shareholders, and the government is accountable to its citizens, but shareholders and citizens are not equal or work at the same scale (Knott, 1993). This extends to critical infrastructure, where private sector security investments react to market forces and commercial incentives, while government investment tends to reflect national security (Auerswald et al., 2005).

Despite their differences, the private and public organizations engage in operation and governance of critical infrastructure (Auerswald et al., 2005). The Solarium Commission (2020) recommended to substantially increase government collaboration and partnership with the private sector, but the Commission acknowledged historical difficulty still exists "because the government is not optimized to be quick or agile" (p. 4), in part due to government requirements for reporting and layers of administration. The US Constitution enshrined this path dependency which will likely affect CSR managers' approach selection.

The impact of organizational challenges on the CSR manager and how to choose risk I&A approaches is a function of their discretion, views on compliance, and degree of ambiguity within cybersecurity policies (Tisdale, 2016). The greater the discretion, the more likely the local setting will determine the implementation. Whether this turns out to be good or bad may go unnoticed in the CSRI&A context unless revealed from an audit or action report after a cyber event. FISMA (2002) required the federal government to fully adopt the NIST RMF. However, despite the NIST RMF offering relatively clear guidance on where and how to consider risk management steps, there is a distinct lack of explicit description for determining levels of risk. The ambiguity might create a challenge or opportunity for CSR managers to identify approaches for use alongside the RMF to fill this gap. For example, Lipner and Lampson (2016) discussed how the RMF should be implemented, scaffolding with other standards along with the NIST Special Publication 800-53. It is not yet clear from the literature if or how CSR managers leverage their discretion when selecting approaches. Information directly from CSR managers could fill these information gaps, but it does not seem anyone has asked them which presents another novel contribution to the scholarship. The last section of this chapter addresses the remaining state-of-the-art gap.

2.6 Spanning the Gap

My research draws from a wide range of domains, such as information systems, risk management, public policy and administration, cybersecurity economics, and organizational studies. Significant work is being accomplished in those fields to create new ways to understand critical infrastructure risk, but there is a research hole between the actors that make approaches, if those approaches are the right organizational fit, determining how much to spend on approaches, how users would learn of or adopt and implement approaches, or how the structural

dynamics from organizations and the policies that govern them affect approach selection. These gaps are important because they have the potential to inform how taxpayers' dollars should be spent to keep the US critical infrastructure safe as well as to expand our understanding, theory, and practice of sociotechnical cybersecurity. Below, I scaffold the literature gaps which informs my work in the areas of human and organizational CSR decision-making.

Selecting CSR approaches is part of a larger plan for cybersecurity strategic resource expenditures and allocation. Cost-benefit analyses, like the Gordon-Loeb model, helped determine economic justification for selecting a CSRI&A approach, and more recent applications by Gordon, Loeb, and Zhou (2016; 2020) showed how the model can be used in conjunction with the NIST CSF. Their work is a cornerstone within the economics of information security, but their optimization modeling focuses substantially on the investment component of approach choice and is sensitive to imperfect information challenges, as well as goal displacement or organizational cheating (Bohte & Meier, 2000).

Overcoming imperfect information benefits from additional and more superior measurement options can lead to better CSR decision-making. Work by Harry (2015) and Harry and Gallagher (2019) take approach development to the next level, where they advance CSR research and methods that consider primary and secondary effects of cyber events. Their work broke ground on new ways to consider, categorize, quantify, and visualize risk that helped build their Tapestry risk assessment technology (Campbell, 2022). As producers of this new approach, they made strong arguments for its use and demonstrated its capabilities. Their justifications focused on the comparative performance and risk measurement aspects, and they did not consider other reasons why a CSR manager might select a different approach than theirs. Tapestry is a bleeding-edge approach and, akin to other complex risk I&A approaches, its expert

consultants recommend their guided implementation, introducing a gatekeeper aspect. The ability to visually break down, process, and resource priorities for cyber risks can be a powerful decision factor for most managers, but Roberto, Bohmer, and Edmonston (2006) noted that even quantitatively oriented teams operate within the preferences of their organizational norms.

Addressing the human element, Haney and Lutters' (2021) work with cybersecurity advocates and Alshaikh's (2020) similar work with cybersecurity champions explored ways in which professionals increase their cybersecurity knowledge, connected with peers, and made decisions. Work in this area described the human realm but not the policy and administrative infrastructural context in which those people work. The policy and administrative stressors that impact decisions are not obvious. Implications and recommendations from this line of research have the potential to help reshape the cybersecurity profession, one type of paradigm shift I mentioned in Section 2.4. However, the guidance may require their own internal or external champions or institutional structures to actualize longstanding organizational change.

Clark-Ginsberg and Slayton's technology studies and policy literature regarding critical infrastructure addressed the association between regulatory policy and cybersecurity risk (Clark-Ginsberg & Slayton, 2018; Slayton & Clark-Ginsberg, 2018). Slayton's (2020) work involved critical infrastructure regulators, specifically of public utility commissions, regarding the development of cybersecurity expertise and sharing specialized knowledge. Atkins and Lawson's (2021) work on critical infrastructure policy and cyber threats existed in a similar regulatory research space with respect to partnerships, competition, and regulatory regimes. However, while this group of scholars linked policy and expertise to threat decisions and critical infrastructure concerns, they did not link these back to discussions about the available or selected approaches that could be used to improve critical infrastructure security. They also did not connect

professional development and policy outcomes back to ways in which CSR managers may encounter and perhaps adopt CSRI&A approaches. This area of inquiry goes a long way to establish interorganizational, operational, external relationships, and sharing expertise between cybersecurity professionals. However, the impact of evidence that information sharing occurs is lessened without knowing if information learned was used later, or at least the intent to use, towards approach selection.

Rounding out this gap, some scholars take a shopping list approach. Research teams at the European Commission's Joint Research Center reviewed 21 risk assessment methodologies used for critical infrastructure which suggested potential target users for those methodologies but fell short by not explaining how the Center's team determined or applied decision factors that paired methodologies to suggested users (Giannopoulous et al., 2012). Moallem (2021) provided a written tour of cybersecurity tools, but it was little more than a descriptive introduction and less a guide to selection as claimed. Ganin et al. (2020) were concerned with the action of decision-making of CSR assessment approaches, yet their work honed into the aspects of the approaches rather than the people that choose those approaches. These scholars addressed an abundant supply side of CSRI&A approaches and made the case for why approaches could be used within a certain context but fell short of my RQs by not answering those questions from the position of the actual CSRI&A managers that selected the approaches.

My work stands on the foundation set by these academics and fills gaps between them. This research connects the scholarly and practitioner communities interested in optimizing approach selection to defend the cybersecurity of critical infrastructure as I explore the human domain and policy elements of approach selection which are necessary in this complex and crowded sociotechnical space.

Table 2:

Summary of Management Space Themes Relevant to the Literature

Section Title / Theme	Core Focus	Key Insights / Arguments	Connections / Contrasts
Drivers of Change in CSR Management	Catalysts and processes of change in risk I&A selection	Focusing events (incidents, policy shifts), technological disruptions, paradigm shifts, rise of new structures, evolving professionalization and standards	Shock vs. gradualism, tech-driven vs. policy-driven, paradigm overlap, co-evolution of context
Organizational Challenges	Internal constraints and conflicts affecting approach selection	Bureaucratic, sector, and staff differences; ambiguity in policy; tensions between standardization and discretion; complexity of public/private organizational goals	Market vs. mission, discretion vs. compliance, sectoral divides, implementation gap
Inter- / Intra-organizational (Re)Action	Organizational responses and networked influences on CSR management	Agreement/friction over risk I&A approach implementation; sectoral incentives, public-private differences, vendor/consultant/academia roles in shaping practice	Cross-sector exchanges, boundary-spanning agents, government/private sector, consensus vs. divergence

In this chapter I introduced three key themes impacting CSRI&A, as summarized in Table 2. A firm understanding of these themes is essential to understand the decision making processes of executive management in these contexts. In the next chapter, I leverage the detailed CSR management space to describe the conceptual framework that I use to help understand the CSRI&A approach selection process.

Chapter 3: Conceptual Framework

In Chapters 1 and 2, I established a CSR management space and discussed elements that may influence how and why specific approaches are selected. In this chapter, I present a novel conceptual framework for the analysis of the selection process. The sections below start with a discussion of key theories that form the foundations for my conceptual framework. I then map those theories to the CSR management space to illustrate where and how they could help explain approach selection, and where each falls short because they address only select parts of CSR management space or have an analytical lens that is too limited to capture the range of reasons why an approach might be selected. I derive that there must be a universal baseline between them that helps explain approach adoption which forms my theoretical framework. Next, I detail the framework and its three constructs, functional differences, and situational differences. Finally, I provide a brief applied example of the conceptual framework to demonstrate its use in the field.

3.1 Theoretical Foundations for the Conceptual Framework

Approaches consist of methods, models, frameworks, guidance, tools, and procedures. For this research, I treat all CSRI&A approaches as formalized practices or systems that may be adopted for use.

There are many useful theories to help explain approach selection in subfields such as information diffusion, decision choice, user acceptance, and organizational structure. All these are useful lenses for technology adoption and an effective way to explore this selection space, as technology adoption processes are inherently complex, sociotechnical learning events, rife with unique perceptions and context (Lai, 2017; Straub, 2009). However, as I will show in later

sections, each of these theories explains only a subsection of the larger selection space of people, organizations, technology, policy, and so on. From them, I create a conceptual framework that captures the entire management space. Coming from varied disciplinary traditions, scholars may use similar terminology, such as technology, in different ways or context.

In this section, I discuss four key theories from subfields applicable to adoption processes: diffusion, decision choice, user acceptance, and organizational structure, displayed in Table 2. All of these areas are well established across multiple disciplines and together create a comprehensive view into the CSRI&A approach choice. Each theory can individually inform various aspects of a cybersecurity manager's experience and relate to the previous literature and selection space, but none seem to explain it completely when viewed independently. Furthermore, I am not choosing one single theory as more advantageous than another because they are all complex and competing, and each offers specific, useful perspectives. Nor do I plan on unifying these theories. Instead, they, along with the literature, will help inform a conceptual framework in following subsections.

Table 3

Theories Informing the Conceptual Framework

Theory Area	**Key Theory**	**Key Scholar(s)**
Diffusion	Diffusion of innovation (DIT)	Rogers (2003)
Decision choice	Rational choice (RCT)	Scott (2000)
User acceptance	Tech. adoption model (TAM3)	Venkatesh & Davis (2008)
Organizational structure	Disruptive technology (DTT)	Christensen & Overdorf (2000)

Diffusion theories focus on the network or environment rather than an individual. Diffusion refers to the adoption of the technology as information about that technology spreads

through an environment such as an organization from person to person or person to system. Arguably, the diffusion of innovation theory from Rogers (2003) is the most well-known, which models how ideas, products, and other content move through a network or system of networks, as well as the momentum of and influences upon that movement. Diffusion of innovation theory (DIT) explains that the CSR manager would adopt an approach via the recommendation of colleagues and upper management within their organization, their security counterparts at interdependent organizations, or from the broader professional institutions. Taking on a network graph structure, in addition to people, organizations can also serve as nodes through their various forms of institutional memory such as knowledge bases that store CSRI&A approach information. Edges can form between nodes through factors like an organization's choice to hire a CSR management consultant or from external policies like those connecting federal agencies. In the latter cases, transmission can come through policy mandates such as the use of the NIST RMF.

Decision choice theories pertain to the motives, preferences, processes, and other influences that lead to decisions about some circumstance or action (Steele & Stefánsson, 2020). In this context, these theories augment and support human decision-making to help determine if a technology is adopted or not. One subfield of decision theory pertains to normative decisions derived from measures of uncertainty and utility and are a way to objectively maximize benefit from a range of possible choices (ibid). Typically, decision-making theories work with a rational orientation and can be considered from the individual and organizational perspectives. One dominant utility-based decision-making theory is rational choice theory (RCT) which uses cost versus benefit analyses applied to alternative courses of action to select an outcome that maximizes self-interest (Ostrom, 2007; Scott, 2000). This process requires a consistent value

system to weigh risks, or other decision outcome options, and determine optimal choices. RCT is common with technology decisions within organizations (Hillmer, 2009, p. 16). CSR managers may use rational choice processes to select approaches because governments typically have strict procurement and other standards that can act as value systems. However, RCT is challenging because complete information for wholly rational decisions is rare, if not impossible, and so adoption by the CSR manager or their organization may need to account for matters of cognitive capacity and satisficing, where satisficed decisions are based on good enough, rather than optimal, outcomes (Simon, 1955). Imperfect information was a quality for drivers of change in CSR management and a key aspect for satisficing.

User acceptance theories stem from well-established information systems and technology literature. Among the more well known is the technology adoption model, currently in its third iteration, TAM3 (Venkatesh & Bala, 2008). TAM3 centers on dimensions of use, perceived usefulness, and perceived ease of use which then influence intention to use and use behavior. In this way, approach selection based on usefulness is like rational choice. Thirteen external variables, to include previous experiences and job relevance, help account for the use dimensions. Unlike the previous two theory areas, user acceptance theories like TAM3 focus on the individual and relegate organizational factors as external variables. Full consideration of these models for CSRI&A approach adoption is problematic in that user accepted theories generally "assume a common understanding and meaning for all individuals involved" (Hillmer, 2009, p. 21). CSR managers are not homogenous and operate within deep bureaucracies and complex interdependent networks, and TAM3 does not account for this sociotechnical influence. CSR managers also exist within diverse professional associations, as witnessed by the large number of certification institutions. Taken together, while CSR managers may share common

CSRI&A end goals, the knowledge, norms, and values may vary greatly and confound TAM3 and similar user acceptance models.

Lastly, organizational structure theories have the advantage of the macro-level selection choice, with a focus on organizational culture and values. A central theme in this group is the replacement of one technology with a newer one, as with disruptive technology theory (DTT) (Christensen & Overdorf, 2000). In DTT, as a technology becomes increasingly established within an organization and entrenched within the organizational culture, aspects of the technology become routine and influential over newer, potentially replacement, technologies. Examples of disruptive technologies either growing in adoption or already entrenched in many modern organizations that affect cybersecurity include cloud computing, which empowers remote data processing and storage, and cryptocurrency as a new type of digital payment (Dupont, 2013; Limba et al., 2019). Incoming technologies must disrupt the incumbent technology, which can happen within a CSRI&A context by way of management consultants or policies that introduce methodological advances in CSRI&A. However, when it comes time to adopt a new approach, others within the organization may remain hesitant or resistive toward accepting adoption. Organizational structure theories tend to ignore the individual, which can be important when it comes to user agency and discretion, particularly within larger organizations and when policy is vague, such as the NIST RMF.

These four areas of key theories have few commonalities in how technology is adopted, such as the degree to which user preference plays a role. More often, these theories diverge, offering different but not incompatible alternatives for CSRI&A approach selection. In the next subsection, I map these key theories onto the CSR management space. Afterwards, these theories will be useful to frame the conceptual framework and later help ground my research questions.

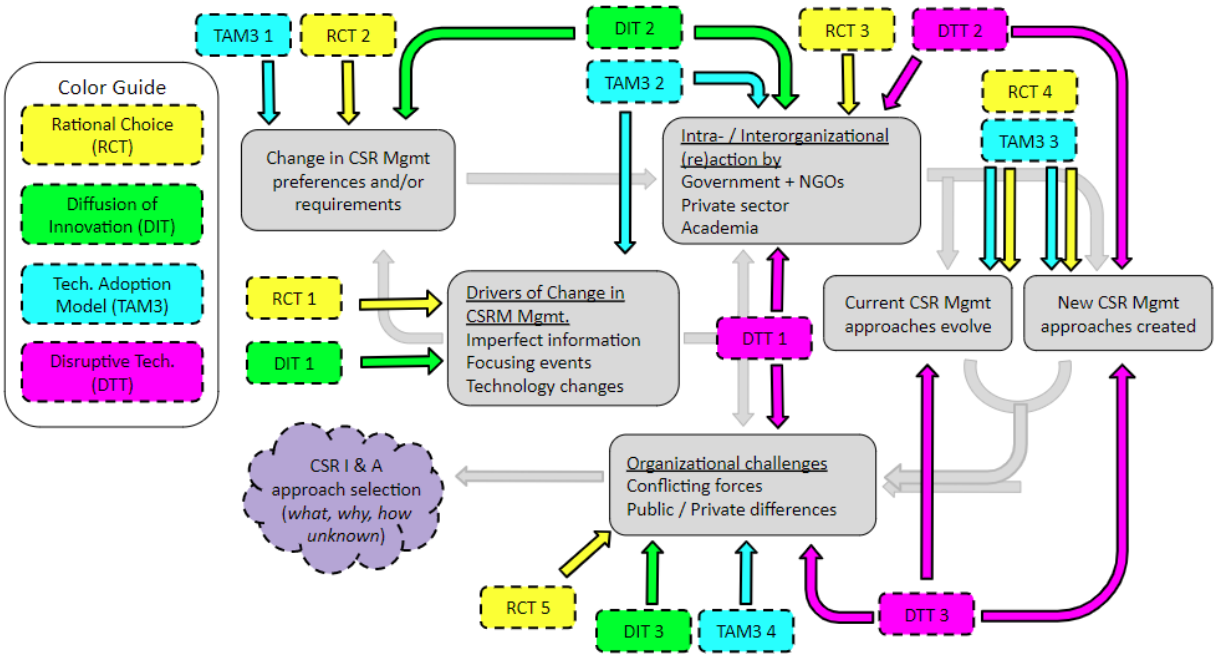
3.2 Mapping Key Theories to the CSR Management Space

In the previous section, I introduced four key theories of technology adoption: DIT, RCT, TAM3, and DTT. Below in Figure 3, I map each key theory to elements in the CSR management space as potential avenues for how each theory might help inform I&A approach selection. In the rest of this section, I explain the numbered theory labels that appear in Figure 3. Theory elements in that figure are color-coded, while other elements of this space are grey.

The approach selection under DIT pertains to network aspects. DIT 1 may inform drivers of change in CSRI&A as network connections are reactionary to events and operate new technologies. DIT 2 may inform changes in I&A aspects of management preferences and/or requirements and intra-/interorganizational elements where network connections (or lack of) are prescriptive. For example, all federal agencies have a mandate to implement the NIST RMF, thereby forging network ties to each other through NIST. DIT 3 also appears alongside organizational challenges as network connections (or lack of) affect the flow of innovations, such as best practices, spreading within communities of practice.

Figure 3

Key Theories Toward CSRI&A Approach Selection within the CSR Management Space



Approaches selected assessed by RCT should exhibit characteristics that attempt to rationally maximize some value. RCT 1 may inform drivers of change in CSRI&A since imperfect information is a key aspect of this element and aligns closely with RCT's similar challenges with cognitive capacity and satisficing. RCT 2 may inform changes in management preferences and/or requirements toward I&A through establishing and exercising explicit value system preferences. These similar values contribute at RCT 4 toward the development of new approaches and evolving other approaches. RCT 3 may observe value-driven selection within the intra-/interorganizational elements when confronted with regulations and similar standards such as means testing. RCT 5 also appears alongside organizational challenges where rational thinking is a common lens used for operations of procurement processes, prediction, and optimization requirements.

Examination using TAM3 relates to selecting approaches based on usefulness.[1] TAM3 1 may inform changes in management preferences and/or requirements toward I&A as these preferences closely align with matters of perceived use and ease of use with an underlying rationale for selection choice. TAM3 2 could offer insight into intra-/interorganizational elements, as well as drivers of change in CSRI&A, as these elements could struggle with heterogeneous forms of management, may have complex networks, and help describe sociotechnical influences. TAM3 3 appears alongside development of new approaches and evolving other approaches because roots for such could be grounded in desires to account for common and aggregated user experiences and organizational demands. This is closely tied to TAM3 4 for organizational challenges through the assessment of behavioral intent to use and use behavior, e.g., social influence, facilitating conditions, and system characteristics.

Lastly, approaches understood through DTT would be responsive to aspects of organizational structure, routinization, culture, and norms. DTT 1 may inform drivers of change in CSRI&A and intra-/interorganizational elements through organizational cultural shifts in preferences and operational processes, e.g., leaning toward routinization of risk. DTT 2 might be useful in development of new approaches and evolving other approaches since the disruption may come from external actors introducing new approaches or ideas for change. Likewise, DTT 3 appears also at new and evolving approaches, as well as organizational challenges, as it might help understanding through an approaches' embeddedness within an organization until it reaches

[1] Theory items here appear to have two numbers, e.g., TAM3 1. The first number is name of the theory, with TAM3 being the third TAM iteration. The second number matches to the theory item numbering, as done by the other three theories.

a tipping point for a new 'best' approach. Each of these theories offers a way to understand the selection, but there may be a better, more useful baseline among them to draw upon.

3.3 Establishing the Conceptual Framework

In this section, I present a conceptual framework that draws upon features inferred from each of the key theories discussed in the previous two sections. Those theories share a common usefulness toward understanding the aspects of adopting CSRI&A approaches. Although each theory accomplishes this understanding in vastly different ways, I derive that there must be a universal baseline between them that helps explain predictive adoption. Because it draws from each of the theories which mapped widely across all the elements in Figure 3, the conceptual framework should be effective when examining approach selection.

The framework has three constructs I derived by reviewing characteristics of each key theory for adoption in this specific context toward affecting CSRI&A approach selection. It is possible that more than three constructs exist or that some may be invalidated or require reframing, which I will discuss further in Chapter 5. First, CSR managers may differ in how they understand the CSRI&A knowledge space, which I define as fundamental understanding. Second, CSR managers may experience functional differences, pertaining to best fit for the problems and more closely related to how CSRI&A approaches are implemented or the resource required. Third, choice may depend on situational differences where there is something in the context for each CSR manager's experience and explains CSRI&A approach selection.

Table 4

Conceptual Framework

Construct	Difference description
Fundamental understanding differences	Definitions and knowledge space
Functional differences	Best for the problem
Situational differences	Context matters

These three constructs of fundamental understanding differences, functional differences, and situational differences comprise my conceptual framework. Each carries assumptions about how CSRI&A choice happens, and it may be that none or all of these constructs are valid. To help further explore the conceptual framework, Table 4 below connects each adoption theory to a conceptual framework construct, offering additional insight as to if and where predictive capabilities based on the adoption theories may emerge.

Table 5

Mapping Theories of Technology Adoption to the Conceptual Framework

↓ Adoption Theories	Conceptual Framework Constructs		
	Fundamental	**Functional**	**Situational**
Diffusion of innovations (DIT)	If we do not share the same language, we are not communicating and not forming / sharing that network tie that would allow for the approach to diffuse.	Network attributes can outline implementation patterns, such as who adopted a particular approach, as well as affect the range of approaches the CSR manager can access to determine which is the optimal approach.	Individual preferences, behavior, and motivations, as well as socio-structural factors and interorganizational dynamics, could affect network tie formation that allow for approach diffusion. Advocates and third-party agents could affect tie formation and championing approaches and other interests throughout the network.

Table 4 continued	**Fundamental**	**Functional**	**Situational**
Rational choice theory (RCT)	If we do not share the same language, we may assign different values for the cost-benefit assessment of an approach, achieving non-optimal results that affect the selection outcome.	Shared concepts of optimal outcomes that are most favorable to self-interests help generate roadmaps by which input criteria are considered, weighed, and lead to selection of a CSRI&A approach.	RCT may struggle with situational context due to the unique aspects of individuals and organizations. Non-rational attributes such as sense of duty or politics can affect other selection measures like risk appetite.
Technology adoption model (TAM3)	If we do not share the same language, we violate the user acceptance theory assumption of "a common understanding and meaning for all individuals involved" (Hillmer, 2009, p.21). So, instruments of TAM3 only work well when language is shared.	CSR managers may have pushback from others in the agency when the individually focused 13 input variables for TAM3 produce a sense of perceived usefulness and perceived ease of use that may differ from what the agency considers as best possible solutions. Moreover, agencies can use bureaucracy, i.e., standard operating procedures, to offset optimal individual choices in favor of optimal organizational choices.	TAM3 would have a lot to say about situational context. Each of the 13 input variables are, by design, meant to help understand usefulness and ease of use, which subsequently help answer the 'is it right for me or the organization', an answer that is often highly contextual.

Table 4 continued	Fundamental	Functional	Situational
Disruptive technology theory (DTT)	If we do not share the same language, adoption or not of disruptive approaches may be associated with the amount of or attitudes toward new jargon to accept.	DTT offers an interesting opportunity to examine the tipping point in an agency as to when a CSR management approach is a satisficing solution to displace any previous approaches or identify pockets of resistance.	The presence of an advocate or third-party agent could affect the chance of selection. DTT closely aligns with situational differences. This alignment is at least in part because of DTT's close association with organizational culture, a focus on the technology change such as CSR management adoption, and the pathway that can help document implementation.

3.3.1 Fundamental understanding differences

First, approach choice depends on the cybersecurity managers' fundamental understanding of CSRI&A. For example, two such managers could agree that concepts like risk, risk management, or cybersecurity are essential to their work, but adopt different CSRI&A approaches if they do not share the same definitions for those concepts. While there might be overall commonality in which CSRI&A terms are important to fundamental understanding, such universal definitions are broadly lacking within CSR management. What definitions existed were not always in agreement or alignment and struggled with poorly established measurement criteria (Ward & Mitchell, 2004). Additionally, differences in fundamental understanding may be systemic as definition variance is widespread and persistent over time. A 2005 Congressional Research Service report revealed challenges with uncertainty surrounding terms and measurement using qualitative and quantitative approaches, as well as pitfalls of where they fail to inform each other (Moteff, 2005).

Epistemological aspects for the fundamental understanding of CSRI&A include discussion that helps answer questions such as ‘what do we know about our cybersecurity and information systems?’ and ‘how do we know our systems are cybersecure?’. The latter is a difficult question, as security is a tradeoff that we are unlikely to take steps to assure complete security at the expense of things like usability. Furthermore, in both questions, CSRI&A methods must attend to elements that could be identified but remain unknowable based on their chance of occurrence or actual impact, and in such places, we proxy these unknowns with risk indicators of elements we do know (Gerstein et al., 2016). Even being able to map entire networks of relationships, the emergent nature of risk systems makes it so that actual risks are never completely known (Clark-Ginsberg & Slayton, 2018).

Each theory of adoption provides a way to examine the CSR management space toward I&A but only captures a portion of fundamental understanding. My expression of the gaps and boundaries here and for the other constructs are simplified. DIT, TAM3, and RCT fall short because it is possible for an approach to be adopted without knowing if the CSR manager shares a fundamental understanding with others that use the same approach. This is typically due to favoring a type of advantage with DIT, RCT, and TAM3’s weakness for high amounts of heterogeneity which occur in this CSR management space due to the prevalence of ambiguity within well-known approaches like the NIST RMF. DTT fairs better toward common understanding due to the strong emphasis on organizational culture and norms which include language and expression.

Using terms differently can send cybersecurity managers off in different directions. Moving in different directions can isolate CSR managers, possibly leading to increased division in language by the size-reduced communities of practice. In turn, this may then require resources

to successfully translate terms when the managers reconnect with individuals that do not share the same language or its meaning. Conversely, such gatherings of CSR managers from different communities can negotiate and standardize language to close gaps in fundamental understanding.

Variation in definitions and epistemology, possibly due to change within the CSR management profession, can lead to inconsistencies in the fundamental understanding of CSRI&A. This spills into development of intuition and forms of internal assessment, learned as part of professionalization, that can influence decision determinants for CSRI&A approach adoption and application (Hubbard, 2009). Complex CSRI&A approaches like OCTAVE or FAIR rely heavily on the expertise of CSR managers, an expertise derived from exercising the managers' fundamental understanding which continues to shape both CSRI&A approach choice and implementation.

Fundamental understanding only requires alignment on terminology related to the CSRI&A approach and its implementation. While fundamental understanding is not concerned with other aspects of the CSR manager's duties, organization, or profession in this context, CSR manager communities of practice form and strengthen when they share a common fundamental understanding. The policy ecosystem creates a baseline community for public cybersecurity managers who must implement the ambiguous NIST risk standards. The revolving door practice of public administrators changes to the private sector, and vice versa, as well as regular engagements through contracting, partnerships, and informal exchanges, allows government baselines of understanding to transfer to their private sector counterparts. This may be of increasing importance for critical infrastructure where much of it is run by private organizations, but regulatory oversight comes from the government. Notwithstanding, the policy ecosystem openly accepts agency flexibility and thus by extension those agency managers (Cyberspace

Solarium Commission, 2020). Here, a cybersecurity manager's fundamental understanding as a lens can help interpret usage of relevant policies toward selecting CSRI&A approaches. For example, if such a manager uses the policies for sensemaking, chosen CSRI&A approaches should reflect the way in which that manager understands the policy. Within these group spaces, it is still viable for these managers to choose different CSRI&A approaches.

Operationalizing fundamental understanding starts with measurement of definitions through asking questions like 'what does risk mean to you?'. This fundamental understanding is achieved through high amounts of congruence between the same definition among different people which can be assessed qualitatively using a codebook and deduction (Cassell & Symon, 2004) or quantitatively with word proximity matching methods such as Jaccard similarity scores (Zhou et al., 2018). Translation can be operationalized through use of examples, analogies, boundary spanning agents, and objects (Star & Griesemer, 1989). Negotiation can be implemented through building up from common understanding on tangential subjects and consensus building. Standardization can be operationalized by discovering the baseline understanding on the topic of interest and benefits from translation and negotiation. However, other dynamics such as interpersonal and interorganizational power-based relations may negatively impact these efforts (ibid). In the next subsection, I discuss how functional differences offer an alternative explanation for approach choice selection.

3.1.2 Functional differences

Second, functional differences are based on the characteristics of 'what works well'. A core assumption of functional differences holds that CSR managers are problem solvers who select the best possible CSRI&A approach to address their problem. CSRI&A approaches do not work when they are insufficient (Harry, 2018) or a failure (Hubbard & Seiersen, 2016). CSR

managers with high levels of discretion or faced with ambiguous policy remain flexible to adopt other CSRI&A approaches when introduced to more effective approaches.

It is critical to account for functional differences when choosing to adapt or create new CSRI&A approaches as those methods can depend on the scope to which current strategies are useful and reduce subjectivity. CSRI&A approaches can be understood, used, and communicated differently based on the application domain (Giannopoulos et al., 2012). CSR management approaches that include I&A such as OCTAVE and FAIR are widely used across organizations, but they reflect general risk I&A methods, compared to other approaches specifically for SCADA systems and critical infrastructure (Cherdantseva et al., 2016). Beyond any specific variations between the CSRI&A approaches, functional differences can aid in determining which of these might be the most advantageous choice or choices. Approaches that offer consideration for resource constraints such as budgetary allowance or stakeholder participatory buy-in also affect choice selection.

Operationalizing for functional differences takes the form of determining what organizational and managerial resources and data are available that can be ranked within a value system. Valid measures should include data, typically quantifiable measures such as financial cost or uptime, for a risk assessment approach. Operationalizing for approaches that do not work well for managers can focus on perception measures and evidence of incorrect or hard to complete risk assessment results.

DIT, RCT, and DTT shine when approximating measures of value with which to prioritize selection options. However, my understanding of these theories is that they all tend to focus on the positive accumulation or replacement of a technology, whereas discarded technologies fall to the wayside with little investigation. Measures of functional differences take

interest in what works and what works well but also addresses the gap of what is not as efficient. This allows for a more complete spectrum of functionality and could help allow for future consideration of returning or repurposing previous approaches as needed.

3.1.3 Situational differences

Lastly, the third construct of situational differences places greater emphasis on explanations from within the cybersecurity manager's specific context that identify CSRI&A approach choice. Situational differences encompass both the human and organizational factors, which are not mutually exclusive, that restrict and guide the cybersecurity manager's approach choice. Other situational factors include what CSRI&A approaches are currently used, if any, as well as what methods are available for potential adoption.

Individual behavior and preferences, as well as agency demands, affect CSRI&A approach choice and introduce a wide range of possible and unique managerial contexts. Some of these variations consider different tiers of CSR managers, motivations, and behaviors. Cybersecurity advocates as influencers, and often non-managers, have a similar, vital role regarding cybersecurity technical changes (Haney & Lutters, 2019).

Pressure from external/third-party influences, such as vendors of CSR management approaches, lobbyists, or policy standards, could generate grossly different situational contexts that affect many aspects of behavior and preferences including selection activities of CSRI&A approaches. These third parties can appear unevenly throughout organizations, such as government agencies and CSR management communities of practice (Grossman, 2012). Vendors and lobbyists have a self-interest in obtaining value from CSR managers, approaching managers that fit the third party's needs or resources. Relationships can form into a reinforcement cycle further differentiating a situational context that can affect approach selection. Standards can be

applied to even these situations, such as through the policy fiat, but this reach has legal and other limits. For example, DoD recently declared contractors, including those working on cybersecurity, as "critical infrastructure", meaning those contractors are essential and required to report to work during the COVID-19 pandemic. However, the policy position does not carry legal authority, and cannot coerce the contractors (Mehta, 2020).

Organizational aspects pertain to structural factors and aggregated activities that are not differentiated to the individual. Agencies have their own norms and organizational cultures that permeate into individual actions including the decision-making process. Socio-structural factors such as organizational culture and group dynamics can affect over-/under-estimates of risk and risk-based decisions; even at organizations with strong data-oriented cultures, these factors can influence the type of evidence and approaches needed to make risk-based decisions (Roberto et al., 2006). Similar agency attitudes can affect the size and prominence of an agency's IT and related cybersecurity group, as well as its leadership and relation to other groups.

Intraorganizational dynamics, such as internal politics, can create additional choice pressures. Survey results from critical infrastructure cybersecurity professionals show these organizational attributes affect things like hardware and software updates, collaboration within and between work groups, training opportunities, and overall dialogue interaction throughout the organization (Parsons, 2018). It stands to reason that CSRI&A approaches would also be affected by these differences. Likewise, agencies that have less strict reporting guidelines or those masked with the classified stamp, have leadership with high confidence in existing security, or leaders that perceive themselves or their agencies as insulated from the full effect of any negative impacts, may avoid overly complicated or costly CSRI&A approaches (DHS S&T, 2018). More broadly, the willingness of an agency to take on risk, or its risk appetite, can also

vary by organization. This appetite can inform types of CSRI&A approaches considered or how strictly those methods are implemented. For example, quantitative CSRI&A approaches can offer greater specificity and sensitivity in their results but are often more complex to implement.

Situational differences are operationalized through a logic of appropriateness (March & Olsen, 2008). What is appropriate is flexible based on the extent of context required for understanding the selection approach space. However, boundary signals should emerge when description of the process wanders into tangential, but non-required actions, ideas, processes, and objects.

The situational differences construct can help address a gap in RCT, since that theory is hampered by imperfect information. The context provided by situational differences remains an imperfect solution but helps to expand options for satisficing as needed. TAM3 offers a great deal of beneficial overlap with this construct, which is advantageous given the validity testing of the TAM suite of theories. However, situational differences expand on TAM3 with organizational measures. Under TAM3, an exogenous variable for managerial support only captures perceptions of aid (as opposed to support) to inform other variables in the model. It does not interrogate this type of support, whereas situational differences aim to ask robust probing questions that can get at indirect measures of support with an example below. While DTT excels at capturing similar measures at the organizational level, situational differences help address the DTT gap at the individual level which is overlooked with a forest from the trees point of view for achieving the adoption turning point.

The following section provides an example application of the conceptual framework and follows with the study design.

3.4 Applying the Conceptual Framework

Using this conceptual framework is a qualitative exercise, relying on rich narrative, response data from interviews and open-ended survey questions. For instance, I provide three synthetic example responses to an interview question and show how each response aligns with a different conceptual framework construct. One question asked during interviews inquires what CSRI&A approaches the manager uses. In this hypothetical scenario, four respondents (A, B, C, and D) all stated they use the NIST RMF, but each used that method for a different reason. Table 6 below offers a review of concepts within the conceptual framework.

Table 6

Aspects of the Conceptual Framework

Fundamental understanding differences	Functional differences	Situational differences
Definitions & knowledge space	*Best for the problem*	*Context matters*
• Not always in agreement (Ward & Mitchell, 2004) • Vary over time & uncertainty regarding measurement (Moteff, 2005) • Use of proxies (Gerstein et al., 2016) • May cause isolation of CSR managers and affect policy interpretation	• No use if insufficient (Harry, 2018) or failure (Hubbard & Seiersen, 2016) for the task • CSR managers are problem solvers; favors discretionary choice • Domain application (Gainnopouos et al., 2012) • General vs. specific (Cherdantseva et al., 2016)	• Individuals & orgs. differ • Mgmt. tiers; bureaucratic insulation (DHS S&T, 2018) • Role of advocates (Haney & Lutters, 2019); third parties and communities of practice • Socio-structural factors toward decision (Roberto et al., 2006)

Respondent A, chose to use the NIST RMF because it is widely utilized across government and industry. It uses a common set of terms that make it easy to understand during

the analysis and compares findings with other companies' cyber risk teams. Reports were understood by senior leadership without clarification requests. This was a perfect fit for fundamental differences given the need to ensure good and accurate communication across all RMF users and those who read reports using RMF language.

Respondent B's response stated the NIST RMF is not only comprehensive, but it is available for free. It is also highly adaptable, yet resource light on the company when compared to many other available approaches. Moreover, the RMF is a complementary approach, meaning that it can be combined with other approaches such as FAIR and NIST 800-53 for a more comprehensive identification and assessment process. Functional difference was the best fit construct for person B's experience because of the focus on organizational efficiency, performance, and efficacy.

Respondent C, who works for the US Federal Aviation Administration, noted the application to continuous monitoring programs but stated that it was chosen by executive leadership to remain compliant with FISMA and Executive Order 13800. Here, the situational difference construct applied because this person works for a government agency, making it part of a select group where the NIST RMF is required. Private companies and state governments might also use the NIST RMF, but may not share the same legal mandates that bind US federal agencies.

Not every case will be so clear. Selection rationales can be complex and multifaceted, as such the conceptual framework constructs are not mutually exclusive. Unions occur when reasons for adoption span more than one construct. Respondent D's reason for using the NIST RMF was the flexible, holistic functionality. It did not take much convincing to have the company require their vendors to adopt the RMF to improve greater cybersecurity within the

supply chain. Since the RMF is so widely adopted, the company's cybersecurity team included the RMF as part of the required job experience. Therefore, new hires excelled immediately because they were already familiar with the assessment tools and lingo. This finding was applicable to both fundamental understanding differences and functional differences. Construct unions allow for more expansive and robust discussion of narratives, such as respondent D linking CSR operations to human resources and staffing efforts. I will explore the conceptual framework constructs and their relationships in Chapter 5 with greater detail using real interview data. In the next chapter, I provide the study design which then leads into my early findings.

Chapter 4: Study Design

Protecting US critical infrastructure is a national security priority and involves cybersecurity risk identification and assessment processes. There are numerous approaches available for cybersecurity risk managers to meet a variety of individual, team, and organizational needs. However, it is unclear how CSR managers research and select which approaches to use and as well as why those approaches were chosen.

This chapter details the study design and methodology I used to address these unknowns and answer the research questions identified in Chapter 1. The study was conducted in two stages: semi-structured interviews and a survey that informed an exploratory study which mapped the research questions to the conceptual framework rather than formal hypotheses. An overview of the study and connections between the methodology and research questions are shown in Table 6 and Figure 4 respectively.

Figure 4

Study Design Flow

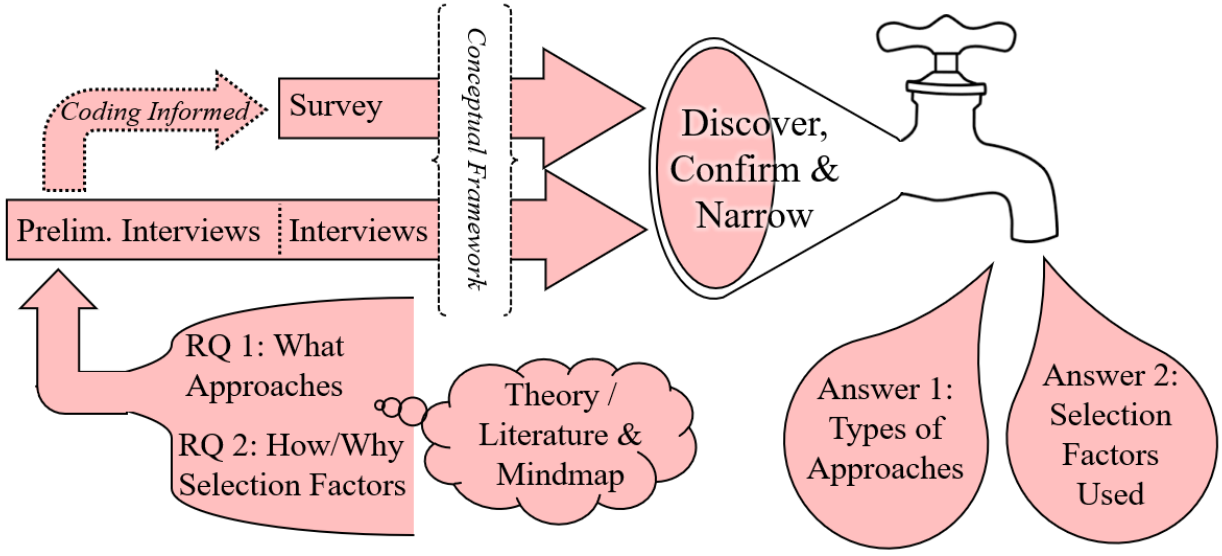


Table 7

Study Design Elements

Interviews		**Surveys**
• Issue identification • Language identification • RQ answer anticipation • Framework testing • Rich detail on challenges and change drivers	*Informed by Interview Coding*	• Explore issues identified • Expand on approach selection factors • Wider range of managerial responses • Highlight sector, managerial-level, and organizational differences

The methods within my study design were the mechanics to determine what findings are most meaningful to generate advice for practitioners and academics. I clustered decision-making processes, sources of learning, preferences, and other response themes across interview and survey data to uncover areas of the greatest and least commonality and impact. In the following chapters, I synthesize the results derived from these methods into guidelines and best practices.

4.1 Interviews of Cybersecurity Managers

The first stage of the study design consisted of multiple interviews utilizing open questions and probing examples to explore the individual and organizational factors related to CSRI&A approaches. The interviews uncovered rich data relevant to both research questions. I used a one-on-one, semi-structured format to acquire a deeper response potential from the predefined questions and flexibility to probe with clarifying questions and natural discussion (Charmaz, 2005; Corbin & Strauss, 2015). The interview materials were approved by the University of Maryland Institutional Review Board (IRB) under Project 1628220-2; refer to Appendix A for the interview guide.

Initial research on CSRI&A approach selection is sparse, so I drew upon methods and questions from related literature that engage cybersecurity and risk management professionals. This literature primarily informed the design of my interview sample and questions. Previous work interviewed cybersecurity professionals to examine their advocacy motivation (Haney & Lutters, 2018), cognitive load and bias as behavioral factors towards cybersecurity products and processes (Pfleeger & Caputo, 2012), the relationship between compliance and security behavior (Haney & Lutters, 2020), and the degree to which critical infrastructure organizations have converged IT and OT cybersecurity planning and implementation (Parsons, 2018). I adapted and built upon the interview questions that appear in Haney and Lutters (2019, p. 116-117), as their questionnaire focused heavily on motivations, challenges, values, estimations for success, and knowledge building, all of which are relevant for cybersecurity managerial decision-making at the upper tiers of management.

4.1.1 Sampling and Recruitment

Respondent recruitment was purposive, consisting of convenience samples based on a three-part sampling frame, detailed in Table 8. The sampling frame served to help pre-screen respondents, ensuring professional experience aligned with this study and maximizing demographic diversity whenever possible. Recruiting started with my own professional connections, those of my associates, and one from a dissertation committee member. Recruitment expanded with snowball sampling of potential participant names provided by respondents, and additional selection occurred through outreach to persons of interest discovered on LinkedIn.

Organizationally, respondents represented both the private and public sectors and quasi-governmental organizations within the US. Most of the US critical infrastructure is owned and

operated by the private sector, while public sector managers may serve as both operators and regulators. Furthermore, "government" for the purpose of this study included federal, state, and local or tribal governments. This multi-sector focus allowed for a comparative cross-sector study. Varying respondents by operator and regulatory functions tiers allowed further comparison and contrast based upon the organization's type of work.

Table 8

Interview Sampling Frame[1]

Frame	**Pool**	**Examples**
Organizational	Public or private US-based organizations responsible for critical infrastructure[2]	US Department of Energy Baltimore Gas and Electric Chase Bank American Airlines
Operational	Have authority to choose which approaches to use. Manager at the Director to C-Suite level.	Director of Cybersecurity Senior Director of Cyber Risk Chief Information Security Officer
Demographic	Maximize on organizational demographics, but sensitive to personal and professional metrics.[3]	Org demographics: Type of organization (e.g., National Laboratory) Infrastructure sector (e.g., Dams) Professional metrics: Years of cybersecurity management experience Amount of responsibility for critical infrastructure cybersecurity

[1] *Table details categorical bins for purposive sample, also serve as pre-screening.*
[2] *Through operation, regulation, or legislation of at least 1 of the 16 critical infrastructure sectors defined by US CISA.*
[3] *Interviewees were not asked to provide their personal identity demographic information.*

Operationally, respondents needed to have some level of authority to adopt or otherwise change the approaches or approach-related policies used as part of their regular CSRI&A duties.

This translated functionally with senior manager interview participants ranging from director and senior director levels on the low end to C-Suite on the high end. I selected participants based on a combination of job duties and titles because exact job titles vary by employer. Due to challenges accessing these individuals, this study also included former managers and consultants that would otherwise meet the sampling frame criteria. Participants on the lower end of the leadership spectrum were more likely to perform risk assessments and engage with IT, OT, and human systems and processes. On the other hand, management at upper levels increasingly engaged in strategic cybersecurity risk identification and assessment decision-making for the organization.

Demographically, I aimed to maximize diversity based on organizational features. However, I remained sensitive to personal and professional demographics and sought opportunities to hear from diverse respondents, since individual diversity tended to provide better collective security efficacy in organizations (Johnston et al., 2019). Demographic data was collected using professional profiles, such as LinkedIn, company website profiles or resumes.

4.1.2 Interview Data Collection

Interviews were conducted from Spring 2021 to Spring 2023. I paused after the first three to review the protocol and obtain a data baseline to assess the conceptual framework. After collecting eleven interviews, I conducted a preliminary assessment of the conceptual framework's performance and identified salient issues for the survey to examine in the study's second stage. Interviews continued until reaching twenty-two, when responses provided sufficiently diminished returns on new information gleaned between interviews.

Due to the COVID-19 pandemic, all interviews took place on Zoom and were approximately 45-70 minutes long, depending on the number of probing questions, clarifying

discussion, and the respondents' interest to share information. Before each interview, participants received a copy of the twenty questions to be asked and a research participation consent form, which included the purpose of the study and details regarding how the interview data will be used and stored. Respondents provided and confirmed consent either by returning the signed consent form prior to the interview or recorded audio of their verbal consent at the start of an interview.

All interviews consented to audio recordings for transcription purposes. Respondent names and their organizations were anonymized unless that participant specifically authorized a quote that would de-anonymize them. I used Otter.ai,[2] an online computational transcription service approved by IRB, to process the saved audio file and quality checked each transcription against its recording to edit errors and anonymize as needed by manually inspecting the transcripts while listening to each interview recording.

The first three interviews served to test the interview protocol, questions, and length. There were no substantial issues, and the overall protocol remained the same. See Table 9 for interview question changes. Early respondents remained part of the total interview data sample. Additional sampling continued until interview response began to data saturate, which occurs as response variation decreases and redundant information increases as the conceptual framework instantiates across the interview data using the deductive coding analysis (Carminati, 2018). Examples of data saturation appeared across participants through response repetition on items such as decision processes, information systems, and sources of learning.

[2] https://otter.ai/

4.1.3 Interview Analysis

This section presents the analysis of interview data, detailing how the instrument was designed and applied in relation to the conceptual framework. Emphasis is placed on the evolution of coding procedures, which were modified in response to emerging patterns and insights from participant responses. These adjustments ensured the analytic approach remained aligned with both theoretical and practical considerations captured throughout the interviews.

4.1.3.1 The Interview Instrument

As mentioned in the previous section, three of the twenty-two interviews served to examine participants' reactions to the questions, how well I understood their responses, and the interview questions' internal reliability. When a question tended to receive uncertainty responses like, "I do not know," probes were added to generate specific information or to answer follow-up questions.

Interview question 14 is an example of an added clarifying probe. This question aimed to reveal names of and supporting information about specific risk I&A approaches used by the cybersecurity manager. Though I stated types of approaches, such as frameworks, software, or management practices, I did not initially name any specific approaches so as not to lead the participant's response. After receiving a couple of uncertainty responses, I added a follow up probe to name approaches such as the NIST RMF, OCTAVE, and FAIR to determine which, if any, were used.

Question nine is an example of an added follow-up probe. The question asked the respondent to describe the last time they conducted a risk I&A. One early response lacked meaningful details that would be useful when coding and another response revealed the respondent did not conduct that type of activity. As a result, I included probing questions when

needed to learn more about the respondent's organization chart which informed the types and duties of cybersecurity managers who may hold additional, useful information.

Table 9

Changes to Interview Questions

Initial	Change type	Revised
(1) Can you tell me about what you do in your job?	Refocus / Rephrase.	(1) How would you describe your job to someone else?
(9) Can you tell me about the time you last did a risk identification and assessment? Please describe what you did.	Added alternate prompt.	(9) Can you tell me about the time you last did a risk identification and assessment? Please describe what you did. *If they do not actually conduct the risk identification and assessment:* Can you walk me through your org chart to a person or team that does risk identification and assessment and tell me what they would do.
(14) *If no specific approaches are named in the last risk identification and assessment, ask the top question; otherwise, skip to first follow-up.* When you did that last risk identification and assessment, what sort of risk methods, models, software, management practices, or other approaches did you use?	Added suggestions as prompt when a respondent did not provide a response or was unsure.	(14) *If no specific approaches are named in the last risk identification and assessment; proceed and ask the top question; if unsure or no response, offer suggestions; otherwise, skip to first follow-up.* When you did that last risk identification and assessment, what sort of risk methods, models, software, management practices, or other approaches did you use? Approach suggestions: NIST-RMF, OCTAVE, FAIR
(17) Are there any other policies, government wide or otherwise, that affect what risk identification and assessment approaches you can or cannot access?	Added additional probe.	(17) Are there any other policies, government wide or otherwise, that affect what risk identification and assessment approaches you can or cannot access? *If affecting external policy was not yet discussed, probe here.* a. How do you see your role and capacity to affect external policy?

4.1.3.2 Analysis and the Conceptual Framework

Using the conceptual framework described in the previous chapter, I iteratively and deductively coded transcripts of the first three interviews using NVivo.[3] This served to determine that the conceptual framework was relevant and applied consistently, and therefore useful toward understanding CSRI&A selection for critical infrastructure. I mapped each construct of the framework using a top-down structure, from the research question to the series of interview questions, to find framework constructs in those interview responses. Participants may contribute responses outside the interview protocol and beyond my intended constructs, in a bottom-up process. Using both these processes, the completed interview response mapping served as the initial codebook by which I identified the extent of the presence or absence of framework constructs. The conceptual framework did not change during this iterative process, although the early application on the interview data helped refine how to conversationally discuss the constructs and their coded findings with my advisor.

The deductive coding was not mutually exclusive. Coding to multiple constructs, such as functional and situational, allowed for more expansive and robust discussions of narratives. Described as unions where multiple construct codes occurred and disunion where they did not, additional interviews may help determine the degree to which unions and disunions represent cooperative activity spaces, such as types of experiences or work practices, and possible tensions between these spaces that might lend themselves to disunion.

[3] https://lumivero.com/products/nvivo/

4.1.3.3 Modification to Early Interview Coding Procedures

My advisor and I worked together through the early interview coding to refine the process. We determined that initial coding was not at the optimal granularity at the question level, so I re-coded the initial transcripts at the sentence level. We reviewed the findings in detail for two transcripts. Our conversations homed in on coding consistency with the conceptual framework. This feedback focused on interpreting the constructs and checking for shoehorn versus natural fit coding. After a few exchanges to improve our internal validity, I coded the remaining transcripts.

Moving through the data, and as an overall quality check on this deductive approach, we discussed if the conceptual framework was sufficient to capture the complexities found in the interview responses. We determined the framework was sensitive enough but also considered the possibility of adding a layer of subcodes, generated through inductive coding, within each construct of the conceptual framework. However, we decided against this, concluding that it would lead the analysis into another methodological direction that did not offer greater return toward answering the research questions. The results of this coding appear in more detail in Chapter 5.

4.1.4 Interview Limitations

Although semi-structured interviews offered rich qualitative findings, there was a notable challenge with data quality and access to respondents. The data quality challenge mattered enough to warrant acknowledgment as it potentially introduced bias into the dataset. The type of bias depended on whether the respondents were a current, internal member of the organization they discussed, or if the overall interview sample was imbalanced, such as an over-abundance of

C-suite to middle-management individuals, or an under-representation of public sector infrastructure operators.

It is possible that some participants had good intentions and responded truthfully but may not have had full access to the current approach selection process at the organization. For example, former cybersecurity managers no longer in that department or at the organization may not be updated on the latest organizational practices, policy requirements, or managerial preferences at their former organization. Alternatively, external consultants sought to guide their management clients, but the consultants did not actually make the approach selection decisions within the organization or had incomplete information as to the organization's needs. In addition, inquiries about compliance and security were perceived as sensitive topics, which possibly introduced non-response bias or social desirability bias into the interview results. Using internal administrative record data to compare alongside interview material was a solution for a more holistic view to overcome this data quality challenge (Amirkhanyan et al., 2018). However, the administrative data was difficult to obtain because no data really exists yet.

Despite these challenges, the potential impact was manageable. Through the purposive sampling frame and completeness determined by data saturation (Francis et al., 2010), I increased the diversity and number of participants until the response data tended toward redundancy and no longer provided unexpected results that might arise from these challenges. Moreover, the population within this research scope reflected a complex environment of systems and people for which transferability was appropriate to the rich interview data (Polit & Beck, 2010), and therefore any potential outliers found in the responses did not have the same challenges as statistical inference methods. Additionally, data quality challenges were offset by conferring with contacts among academia and communities of practice for quality-control

feedback on anonymized interview response snippets. Despite these challenges, attempts to generalize or transfer this research recognized this work had a US-centric scope of critical infrastructure, organizations, and cybersecurity and risk I&A policies.

Lastly, access to people of interest and interpretation were a limitation. It took much longer than anticipated to recruit participants during the initial portion of my interview sampling. A challenge I encountered early on was that it is difficult to find contact information for cybersecurity managers without first having a social network connection to those individuals. Unanswered email outreach, which was common, compounded the matter. Feedback from colleagues and early stage advising respondents noted outreach non-response might have been due to concerns, such as hesitancy or distrust, to the discussion of risk and cybersecurity issues perceived as sensitive. Another theory pertained to barriers from within the potential participant's organization, such as pre-approval requirements from upper management or legal staff. At other times, access difficulty included interpreting consultant responses, as they were at least one-step removed from the organization and people selecting the approaches. This difficulty compounded when consultants referred to different anonymous clients in their responses instead of using one client consistently. I lessened these difficulties by leveraging connections from previously interviewed participants and through professional associations that helped promote and distribute the survey portion of this study design.

4.2 Survey of Cybersecurity Managers

Supplementing the interview data, I conducted a survey of cybersecurity managers followed by statistical analysis of the survey responses. Surveys utilized a well-documented social science method to collect targeted data on behavior, values, and preferences (Fowler, 2013). They captured cybersecurity knowledge and readiness levels which depend upon public

policy decisions (Norris et al., 2019), as well as information strategy and risk assessments of state government level cybersecurity professionals (Deloitte & NASCIO, 2016; Deloitte & NASCIO, 2020). Moreover, surveys were opportunities to connect novel areas of research to problems. For example, the effects of cyber events on critical infrastructure such as dams (U.S.A. v Fathi, 2016) were exacerbated due to the low uptake of and under-resourced cybersecurity training and hygiene (Prall, 2017); yet it was also an opportunity for cybersecurity advocates to help motivate adoption of positive cybersecurity practices (Haney & Lutters, 2019). My survey sought to uncover patterns and policies related to approach selection and its process.

Survey question development occurred through two convergent methods. First, interview questions and responses formed the basis of key topics that were made more specific as to develop close-ended questions tied directly to the research questions. For example, the interviews included one open response question about what CSRI&A approaches were used and another for how they came to select that approach; in the survey, these questions combine into a single question battery of named approaches derived from the interview responses, literature, and expert advice. This question mapped to RQ1 regarding what approaches are used. This process incorporated Landoll's (2011) guidance to develop information security survey questionnaires from interview content and carryover issues such as assessment methods, scope, and budget. The second method of question development sourced survey questions from previous research. This method was used as much as possible as these surveys benefited from field application, review processes, and publication. In most cases, sourced survey questions required minor modification to specify the user or target group to better fit this study. For example, question 3 from the Norris et al. (2019) survey asked, "Does your local government outsource any of its cybersecurity functions," in which I replaced "local government" with "organization" to be

inclusive of participants from various tiers of government and the private sector. That modified question mapped to RQ2 regarding why and how some approaches are selected. Language for questions using this method pull largely from sources in Table 14. Appendix B contains the survey questions and example survey question mapping from the literature.

The survey questions evolved over three iterations of pilot testing, including reviews from two University of Maryland faculty members with cybersecurity and risk expertise, three doctoral students, and three practitioners from industry, two of whom also served to pilot the interview questions. Unlike the interview data, I discarded survey pilot test results, in part due to more extensive changes in question wording, order, and number of questions.

4.2.1 Sampling and Recruitment

For this portion of the study, I surveyed 274 mid-to-high level cybersecurity managers, which I reduced to 216 after data cleaning. Sample size was based on three factors. First, the size remained consistent with previous survey research of cybersecurity management or critical infrastructure professionals (Deloitte & NASCIO, 2020; Norris et al., 2021; Parsons, 2018). Second, with the goal to include representation of all 16 of CISA's critical infrastructure sectors and consideration that 15-20 survey respondents are an appropriate sample size per sector (Harry, 2020), it stood to reason that I only needed 250 survey participants. Third, an n of 250 is more than sufficient for statistical analysis of contingency tables to compare use and preference patterns, given a power of 0.8, Cramer's V medium effect size of 0.3, alpha of 0.05, and degrees of freedom ranging from 2 to 20 (n= 108 to 233 respectively depending on degrees of freedom). To obtain these survey respondents, I used a combination of invitations sent through personally affiliated channels and professional networks as well as leveraging a market research company.

4.2.1.1 Survey Invitation to Participate Through Personal Outreach

Access to the populations of interest typically involved a gatekeeper agent. Norris et al. (2019) partnered with International City/County Management Association (ICMA) and Parsons (2018) partnered with CFE Media to access their engineering magazine publication database. Hatcher et al. (2020) leveraged city websites to obtain address information to build their own contact database, but that option was limited here due to the non-public nature of my target population's contact information. My initial survey outreach was through Information Analysis and Sharing Centers (ISAC), whose membership mailing lists could directly reach a sizable amount of my target population. I reached out to the 27 ISACs listed by the National Council of ISACs using contact information on individual ISAC websites and my previous connections. However, only two ISACs confirmed forwarding my survey participation invite to their members, and another four ISACs mentioned approving my request but not if the invitation was disseminated. Seven ISACs declined my request either based on policy grounds not to use their mailing lists for external solicitations of any type or having received too many similar requests, while the remaining ISACs either did not respond or ceased responding after initial email exchanges. Table 10 lists my ISAC outreach results.

I supplemented this outreach through cybersecurity accreditation and professional development associations, such as ISACA where I hold a membership and accessed my local leadership to assist in survey distribution. I also included general social media posts on LinkedIn and Twitter, as well as through the Wee Dram[4] – an invite-only social-professional group of

[4] This is a private, unlisted group on LinkedIn with viewership only given to group members and membership only provided through recommendation by a current member. They are part of my professional network and background detailed in my positional statement in Section 4.3.

which I am affiliated and consists of largely national defense and cybersecurity leaders who are both potential respondents and other cybersecurity management network gatekeepers.

Organizations were incentivized to assist with survey recruitment by allowing them to add a question to the survey so long as that question was relevant to the overall research topic, did not require respondent's sharing sensitive information, and followed IRB acceptable research conduct standards. Despite the offer, none of the organizations took any interest in adding additional questions, sending the invite as-is. Respondent gratuity was not offered to avoid complications for public sector participants who are unable to accept gifts and the potential for imbalanced incentivization. However, as a thank-you, participants had the option to sign up for a complimentary executive summary of this research post-dissertation completion.

Table 10

ISAC Outreach

Outreach Status	ISAC
Confirmed invite Sent	Automotive (Auto-ISAC), Maritime Transportation System (MTS-ISAC)
Approved invite but unclear if sent	Election Infrastructure (EI-ISAC), Manufacturing (MFG-ISAC) Space (S-ISAC), Water (Water-ISAC)
Declined invite request	Aviation (A-ISAC), Electricity (E-ISAC), Emergency Management and Response (EMR-ISAC), Financial Services (FS-ISAC), Media & Entertainment (ME-ISAC), Real Estate (RE-ISAC), and Retail & Hospitality (RH-ISAC)
Non-response, at all or after initial emails	American Chemistry Council (ACC-ISAC), Communications (NCC), Downstream Natural Gas (NDG-ISAC), Health (H-ISAC), Multi-State (MS-ISAC), National Defense (ND-ISAC), Oil & Natural Gas (ONG-ISAC), Research & Educational Networks (REN-ISAC), Surface Transportation (ST-ISAC), Public Transportation and Over-the-Road Bus (PT & ORT-ISAC), Heathcare Ready, Information Technology (IT-ISAC), Maritime Transportation Security (MSC-ISAC), Small Broadband (NTCA)

The survey sampling frame was like interview recruitment; all participants had to qualify as managers whose duties included some aspect of risk I&A for the cybersecurity of critical

infrastructure with the ability to choose or influence others regarding approach selection. Participants self-selected their organization as private or public sector from a range of subtypes, as well as their organization's critical infrastructure sectors as categorized by CISA. A key difference was expanding the band of management so that participants identified in a middle- to middle-upper tier of management, such as Division Chief or Senior Manager level positions, as well as the upper-tier leadership sought for the interviews. Widening the management sample pool enabled study of those respondents who often share the dual responsibility of implementing directions and strategy from the executive leadership while also interpreting operational work and developing reports for executive leadership.

4.2.1.2 Survey Invitation to Participate Via a Market Research Company

Response turnout through the initial outreach venues went poorly, generating fewer than 30 responses after three months of repeated email and social media posting. Relying on third parties to reach their contacts reduced my ability to determine where, when, and how often follow-up invitations could be sent. It also limited my ability to determine non-response rates or strategies to increase response based on electronic format outreach efforts, such as email opens or bounce patterns, click rates, and adjusting the invitation message designs.

In consultation with my advisor, we determined it was acceptable to hire a market research company to assist with participant recruitment rather than wait the additional time for the initial outreach strategy to slowly meet necessary sample size. After reviewing seven companies, I hired Slice Market Research (Slice MR).[5] Osterman Research, who produces practitioner-oriented cybersecurity, data protection and information governance research and

[5] https://slicestrategy.com/

consulting, recurringly use Slice MR for their data collection needs and provided a personal introduction. Slice MR also made the most convincing case for having access to this study's niche target population through their association-driven recruitment and identification verification methods.

Participant recruitment varied from the previous outreach efforts in that no additional parties were offered an opportunity to add survey questions. Additionally, Slice MR paid participants on a per-person basis at the same rate. The survey sampling frame remained the same; although, the question order and consent process changed as detailed in the next section.

4.2.2 Survey Data Collection

There were two versions of the survey due to the two participant recruitment strategies, the first version for the personal and association outreach efforts and the second for those recruited by Slice MR. Both versions were conducted entirely online via Qualtrics and collected in March and April 2023. The first version was part of invitations to participate sent via email, in accordance with common modern survey research practices (Dillman et al., 2014; Fowler, 2013) or linked posts on social media. When possible, this outreach included addressing emails with the email owner's name and tailored requests to participate. The second version used similar invitation to participate language, but Slice MR delivered it via their own internal survey panel member account and outreach systems.

Both survey versions allowed for independent storage of response data wherein participant names were not linked directly to survey responses. The first version with my recruiting efforts used three separate Qualtrics surveys with the first survey collecting participant consent and its end message linking to the main survey, and then the main survey end message linking to the third, optional survey to sign-up for the post-research executive summary. The use

of three, interlinked surveys allowed me to collect participant names and email addresses in isolation from their survey responses thus increasing participation anonymity. The shared link to the survey was the consent form survey, so participants completed the consent form before proceeding to the main survey.[6]

The Slice MR version included the consent form as part of the main survey, requiring participants to click a positive consent affirmation button rather than provide their name, as Slice MR policy prevented me from obtaining individual names without additional cause. In place of individual names, Slice MR provided a unique individual identifier key which Qualtrics automatically logged with each participant. The identifier key further anonymized participants by design from their survey responses. The change to a button-based consent approval then served as a participation qualification filter in Qualtrics, ending the survey early for anyone who did not affirm consent. As with the first version, Slice MR sourced participants also received the follow-up optional survey to obtain the post-research executive summary. Since the executive summary sign-up was optional and not tied to the main survey, Slice MR approved its use.

Both survey versions included language in the participation invitation for people to self-identify if they qualified, e.g., being at the mid-to-executive level of cybersecurity management. However, the survey versions differed slightly with respect to enforcement of participant qualifications. The first version accounted for qualification initially by only sharing the survey link with individuals who were known to be qualified through personal connections, association

---

[6] The survey contained: one participation consent form, four introductory questions about the manager and their organization, three-to-five questions about what approaches they use, one large question block about approach importance (60-item Likert battery), three quick organization background questions, six quick individual demographic questions, and one final question about for anything else the manager wanted to share. See Appendix B.

membership status, and similar distinguishers. When the links to the first survey version were later shared publicly online, such as on LinkedIn, I closely monitored Qualtrics for low-quality responses, potentially from bots; yet only four low-quality entries made it past the consent form and those were removed during data cleaning. Given the cash payment aspect with Slice MR, I more strictly enforced participant qualification by reordering select questions, such as managerial level or RI&A job duties, to appear on the first page of the survey and thus doubled as participation qualification filters. Like consent, anyone who did not meet the minimum qualifications exited the survey early before reaching the main survey questions. Slice MR did not charge or count toward my contracted sample quote any individuals who exited the survey due to qualifications or data quality control purposes.

4.2.3 Survey Data Cleaning

With 274 survey respondents, I exceeded the 250-person general goal. Post-data cleaning, the sample size dropped to 216 (78.8%) but remained well above the power-test minimums discussed in Section 4.2.1. Data cleaning criteria varied slightly based on each survey type. For the first survey, shared through the ISACs and professional networks, I discarded four of 19 participant records (21%). This choice included those whose entries did not contain responses to key survey questions: which approach they used, description of their selection process, or how they derived custom approaches after indicating they used custom approaches. I also dropped respondents who did not finish the survey or had duplicate IP addresses. There were no issues with meta-survey values such as total response time or effort reporting.

Cleaning the Slice MR survey version was more extensive. I dropped 21 of the 255 respondents (21%) mostly for meta-survey data quality concerns such as values that did not include individuals pre-filtered by Qualtrics for not meeting the minimum sampling frame

participation criteria: consent, minimum age of 18, managerial level, duties that included choosing RI&A approaches, belonging to a critical infrastructure sector organization, and belonging to a US-based organization. I further filtered out participants who indicated being in the US but whose geo-coding listed them outside the US, duplicate IP addresses, and those who completed the survey in less than five minutes.

To assist with data quality controls, Slice MR rolled out the survey in three waves of 29, 30, and 194 participants respectively. Based on early concerns of insufficient effort reporting after the first wave, Slice MR allowed the addition of two attention check questions. The first attention check question required the participant to type in the word "red" and I accepted all three letter case versions received: red, Red, and RED. The second attention check question required the participant to select the number "2" on a 7-point Likert response scale.

Insufficient effort reporting (IER) metrics helped identify participants that were more likely to have randomly chosen or careless response patterns on the long battery of statements with Likert scale responses (Denison, 2022; Hong et al., 2020). Following guidance from Brühlmann et al. (2020) that many IER metrics do not have hard cutlines, I used four IER metrics and standard outlier detection techniques, such as values outside inter-quartiles ranges, box and whisker plots, and quantile thresholds to find extreme values in response patterns. I flagged participants for further investigation if they exceeded soft limits on at least three of the four metrics. Metrics included were longstring values to show the frequency of consecutively identical responses and intra-individual response variability assesses the consecutive item response standard deviations (Dunn et al., 2018). I also used person-total correlation and Mahalanobis distances as other distribution deviation measures, which are also useful for detecting non-human responses (Dension, 2022; Dupuis et al., 2019).

4.2.4 Survey Analysis

Analysis of the survey data informed and validated the conceptual framework and helped explore non-causal relationships between the topic variables and the framework constructs; see Appendix B and Appendix D for the topic and framework mapping. Analysis occurred using R and Excel, focusing on univariate and bivariate patterns, with and without filtering on third variables. Additionally, I applied association rules, a data mining technique, to uncover larger multivariate patterns and other measures of association, which I use to develop approach selection profiles. The work built upon the interview responses confirming or rejecting narratives and built out new responses of interest. As the data is cross-sectional and this study does not focus on inferential hypothesis testing, achieving statistical generalizations beyond the collected sample is not a concern. Previous research discussed in Section 4.2.1 similarly describes limitation of analysis to descriptive statistical findings. The one exception is Hatcher et al. (2020), who used the Chi-Square test of independence to assess relationships found in bivariate tables.

4.2.4.1 Association Rules Primer

Association rules are a data mining technique for discovering interesting descriptive relationships between variables. This technique started in marketing and marketing research, where it is also known as market basket analysis, and spread to informatics, social networks, and wide range of life and physical science disciplines (Aguinis et al., 2013). Application of association rules in cybersecurity initially appeared in intrusion detection systems research (Yanyan & Yuan, 2010) and branched out to other areas of cyber threat intelligence (Abu et al., 2021) and security by design configuration (JohnPaul & Nwalozie, 2024).

Using association rules using a grocery sales context begins with initial concepts where an item is a single product or object, such as bread, jelly, peanut butter, cereal, and milk in a grocery store. Grouped items create itemsets; for example, bread and jelly together make an itemset of two items, while bread, jelly, and peanut butter make an itemset of three. A transaction contains all items from a grocery store purchase, and there are $2^n - 1$ different itemset combinations within the transaction where n equals the number of items in that transaction.[7] Thus, a transaction containing bread, jelly, peanut butter has 7 potential itemsets, with each itemset written with the standard curly brace notation: {bread}, {jelly}, {peanut butter}, {bread, jelly}, {bread, peanut butter}, {jelly, peanut butter}, and {bread, jelly, peanut butter}.

Association rules are formal statements meant to show relationships about and between itemsets across transactions in the data. *Support* is the most basic measure, where expressing a single itemset of interest as X, the formula for *support* is written:

$$\text{Support (X)} = \frac{\text{number of transactions that contain itemset (X)}}{\text{total number of transactions}}$$

Association rules use if-then statements to explore relationships between itemsets. Assigning X and Y as itemsets with non-overlapping items subset from the list of all possible items, the notation $X \Rightarrow Y$ has itemset X on the if or left-hand side and itemset Y on the then or right-hand side; the left-side and right-side itemsets are also called antecedent and consequent respectively. The if-then probabilistic logic of $X \Rightarrow Y$ follows that if itemset X occurs in a transaction, then itemset Y also appears in the same transaction with some likelihood.

Each rule represents a different 'if X, then Y' scenario in the dataset. Thus, returning to the grocery example, one rule examines the chance that if someone buys bread and jelly, they

---

[7] The formula subtracts 1 to remove consideration of the empty set in which there are no items.

also buy peanut butter, whereas another rule examines the likelihood that if someone buys cereal that they also buy milk.

Association rule metrics help uncover patterns that are stronger than random chance. Continuing with $X \Rightarrow Y$, the strength of these rules is typically measured by *support* (the proportion of transactions containing both X and Y), *confidence* (the conditional probability that Y occurs given X), and *lift* (how much more often X and Y occur together compared to what would be expected if they were independent). Mathematically, these measures are written:[8]

$$\text{support}(X \Rightarrow Y) = \frac{\text{number of transactions with both } \{X\} \text{ and } \{Y\}}{\text{total number of transactions}},$$

$$\text{confidence}(X \Rightarrow Y) = \frac{\text{number of transactions with both } \{X\} \text{ and } \{Y\}}{\text{number of transactions with only } \{X\}},$$

$$\text{lift}(X \Rightarrow Y) = \frac{\text{confidence}(X \Rightarrow Y)}{\text{support}(Y)} = \frac{\text{confidence}(X \Rightarrow Y)}{\frac{\text{number of transactions with only } \{Y\}}{\text{total number of transactions}}}$$

To identify rule metrics, I use the Apriori algorithm, one of the most common association rule mining methods. It operates on the principle that any subset of a frequent itemset must itself be frequent. The process begins by calculating the *support* for each individual item in the dataset and discarding those below a user-defined minimum support threshold.[9] The Apriori algorithm then iteratively combines frequent itemsets into larger candidate itemsets and prunes those candidates whose subsets did not meet the minimum support in previous steps. This systematic pruning greatly reduces computation by eliminating unlikely itemsets early. Once all frequent

[8] The association rule formulas I use rely more on words than symbols to help avoid confusion caused by inconsistent notation, especially with union and intersection symbols, which are often used differently across research papers and support forums. See also: Aguinis et al. (2013), Dino (2022), ScienceDirect (2025), and Tan et al. (2018).

[9] Thresholds are defined further in Section 5.3.5 with the association rule findings.

itemsets are identified, the algorithm constructs association rules from these groups and evaluates them using metrics like support, confidence, and lift to discover patterns and relationships in the data.

For this research, I apply association rules to the survey results to find itemsets of managerial and organizational traits that pair with selected approaches. Emergent multivariate patterns from those pairings then become profiles I construct to discuss CSR manager characteristics for those approaches. These methods and discussion continue in Chapter 5.

4.2.5 Survey Limitations

Prior work from similar areas of cybersecurity research have categorically suffered from low response rates despite topics of grave public and private importance. According to Norris et al. (2019) and Norris and Reddick (2013), this is likely due to failed attempts to survey this population—a group that regularly contends with the problems of potentially sharing sensitive information, who are often overworked and under-resourced, and who are inundated with other survey requests. This research also suffered from extremely low participation rates during the first outreach strategy, although it was not possible to pinpoint the exact response rates. Participation challenges were a non-issue via Slice MR, and the sample obtained limited by self-funded resource limits, but there was less certainty of reaching the target population. Overall, the sample size did not impact the diversity of the participants or their meaningful results, but as with previous similar research, care should be taken with generalizing beyond the sample pool. Both recruitment modes have the potential for selection bias but for different reasons given motivation to help the profession and interest in the executive summary in the former strategy, while the latter included financial compensation with Slice MR. Data analysis revealed some

variation comparing survey responses collected from each group, but those results were not significant substantively or statistically.

4.3 Positional Statement

As a social scientist and management professional with over a decade of academic and applied experience in cybersecurity, public administration, and policy, my research perspective is shaped by a deep engagement with both theory and practice. My background includes extensive work with government agencies, nonprofits, and international organizations, where I have led research projects on sociotechnical cybersecurity risk, information security behavior, and strategic decision-making in complex environments. Through roles as a faculty member, research fellow, and consultant, I have developed expertise in advanced quantitative and qualitative methods, program evaluation, and policy analysis, regularly synthesizing literature and data models for both academic and practitioner audiences.

My research, teaching, and service activities have provided me with opportunities to engage with a wide spectrum of cybersecurity professionals, ranging from consultants and technical specialists to C-suite executives. Through organizing and leading a sociotechnical cybersecurity speaker series and insider risk workshop series, I have facilitated dialogue among practitioners and scholars, deepening my understanding of real-world challenges and emerging trends. My collaborations with CERT teams and my experience conducting information security research for national defense and the intelligence community have further broadened my perspective on the operational and strategic dimensions of cybersecurity. As a result, I will occasionally draw upon these prior experiences and professional relationships as sources of subject matter knowledge and context, which inform my interpretation and assessment of data throughout this study.

Chapter 5: Findings and Discussion

With the groundwork laid in the earlier chapters, I present the core results of the study, beginning with a description of the study participants—their backgrounds, roles, and organizations—to provide context for the findings. Next, I address the main research questions: first, what cybersecurity risk identification and assessment approaches managers chose (RQ1), and second, why they made those choices (RQ2). By presenting patterns and explanations from both interviews and surveys, I aim to illustrate how real-world decisions are made and what factors matter most for cybersecurity managers in US critical infrastructure.

5.1 Study Participants

Understanding the sample data is essential for discussing the two research questions. The breakdowns inform representativeness and allow for analysis of interesting subgroups. This section presents findings of the 22 interview and 216 survey participants. Although respondents were required to be current or former cybersecurity managers versed in risk identification and assessment, there was substantial diversity among them. Some held their current roles for less than a year, while others were external consultants. This diversity provided a wider range of responses but also required additional probes during interviews to ensure consistent context and uncover limitations consultants might face compared to internal management. These probes led to survey questions being phrased differently than in the interviews to accommodate the distinct mediums while still yielding diverse results.

Data in this section focuses on participants' individual and organizational demographic information. The purposive sampling strategy intentionally selects for moderate-to-high diversity by organizational demographics such as type of organization, role, and infrastructure sector,

which is vital for cross-institutional analysis. While purposive, the sampling did not include stratification or quota requirements. Data used in this analysis are primarily self-reported by interview and survey participants. When I knew the participant by name, as with the interviews, I sourced supplemental education and employment data from LinkedIn profiles. The following subsections split into individual and organizational measures.

5.1.1 Individual Measures

The following section presents results focused on individual study participants, examining their experiences, perspectives, and decision-making for CSRI&A activities. After this analysis of individual measures is a subsection on organizational-level findings.

5.1.1.1 Managerial Level and Experience

Cybersecurity management measures were grouped into three increments representing early, mid, and late career timelines. Roughly two-thirds of participants had more than 10 years of cybersecurity management experience (70% survey, 63% interview). Among interviewees, the distribution was evenly divided between those in executive C-suite positions and other upper management roles such as senior directors or vice presidents. In the survey group, nearly 60% were middle managers, with another third identifying as upper management and the last 6% as executive level. Table 11 provides greater detail on the distributions of management level and years of experience.

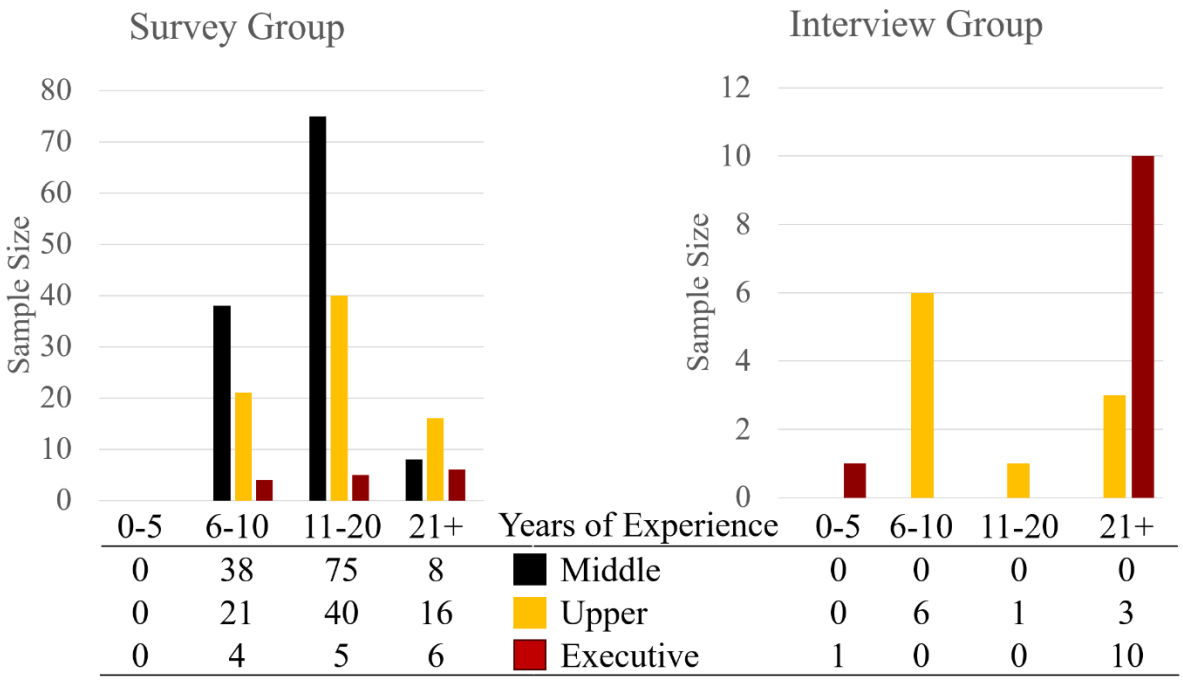
I inferred that the mid and late career groups were familiar with the field, trends, and demands of cybersecurity management, which benefited this study and aligned with the sampling frame intent. About a third of the respondents operated as consultants. While consultants may not be direct decision-makers in choosing CSRI&A approaches, their influence can be significant

based on their relationships with clients. The role of vendors, including consultants, was a key point discussed in the sections below.

Additional background information from the interview data showed that almost three-fourths of respondents worked at private companies (72%), and half were former government managers. Experience in both the private sector and government was not surprising, particularly at higher management levels, as the trend of managers moving between the private sector and government is well-documented (National Conference of State Legislatures, 2021; Summers, 2022).

Table 11

Manager Level by Years of Experience



Survey Group					Interview Group			
0-5	6-10	11-20	21+	Years of Experience	0-5	6-10	11-20	21+
0	38	75	8	Middle	0	0	0	0
0	21	40	16	Upper	0	6	1	3
0	4	5	6	Executive	1	0	0	10

5.1.1.2 CSRI&A Duties

As part of the survey participant qualification, individuals answered if their cybersecurity management duties include performing and/or choosing RI&A approaches or if their work did not include either of those duties. Only survey respondents involved with RI&A approach choice

qualified and among them, approximately 84% of the respondents both choose and perform RI&A duties, and nearly 64% and 29% of this subgroup performed those duties frequently or regularly respectively. This suggests that most cybersecurity managers often involve themselves with operational aspects, as well as strategic planning elements of RI&A activities. Table 12 and Figure 5 show these patterns in greater detail.

Figure 5

Percent of Managers with CSRI&A Duties by Frequency of Those Duties

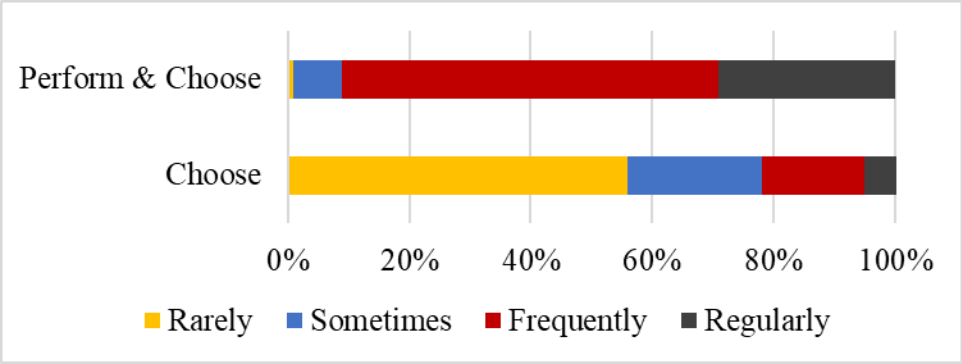


Table 12

Number of Managers with CSRI&A Duties by Frequency of Those Duties

	Not at all	Rarely	Sometimes	Frequently	Regularly	Total
Perform & Choose	0	2	14	114	53	183
Choose	0	10	4	3	1	18
Missing	0	0	2	2	11	15
Total	0	12	20	119	65	216

Table 13

Interview Participant Highest Degree

Degree	N	%
Bachelor	2	9%
Master	13	59%
Doctoral	6	27%
Unknown	1	5%
Total	22	100%

5.1.1.3 Education

Respondent education offers potential inroads to understand managers' formative background, where differences in level of education and focus of study could serve as a lens into how they interpret and perform their managerial work. Interview respondents were overwhelmingly well-educated with 86% having a master's or doctoral degree, compared to 29% of survey respondents. Assuming graduate education may be a motivator for promotion (Ramezan, 2025),[10] this lower percentage for survey respondents is not surprising given the much higher prevalence of middle managers and those having fewer years of experience.

Survey respondents self-described their higher education major fields of study. Typically, they listed only one major, such as computer science or engineering, disassociated from their degree information. Conversely, interview participant education data came from their LinkedIn profiles, which in most cases clearly listed the degree and major subject. This paired education revealed that most (59%) of the interviewees had multiple degrees in different areas of study, such as having a bachelor's degree in English language and literature as well as a master's

[10] Ramezan's 2025 assessment of open CISO positions, showed over 41% listed a master's degree, while just over 1% listed a doctorate. A master's usually reduced required years of experience, while a having a doctorate did not.

degree in cybersecurity and another master's degree in government. Thus, it seems the interview respondents, on average, could draw upon a wider range of academic study to inform their decisions. Unsurprisingly for technical management, the most common major for about two-thirds of survey participants was computer science / IT. Nearly 15% of respondents were split evenly between data / information science and business degree-type majors, with several other majors listed once or twice. Although nearly 7% did not share a degree major, all but two of them identified having an Associate degree where a major might not be applicable. Additional highest degree and fields of study for interview and survey participants appear in Tables 13, 14, and 15.

Table 14

Interview Participant Higher Education by Major

Major*	N	% of 22 Part.	% of All Majors	Major* (con't.)	N	% of 22 Part.	% of All Majors
Business	6	27%	16%	Strategy	3	14%	8%
Computer Science (CS) / IT	6	27%	16%	Communications	2	9%	5%
Engineering	3	14%	8%	Govt. & Public Administration	2	9%	5%
Language	3	14%	8%	Criminal Justice	1	5%	3%
Math & Stats	3	14%	8%	Economics	1	5%	3%
Physics	3	14%	8%	History	1	5%	3%
Political Sci. & Intl. Relations	3	14%	8%	Total	37	100%	100%

Note: * Self-identified majors were grouped into common areas of study listed here.

Table 15

Survey Participant Higher Education by Major and Highest Degree

Major*	N	%	Associate	Bachelor	Master	Doctoral
Computer Science / IT only	142	65.7%	0	94	47	1
Data/Information Science	16	7.4%	0	12	4	0
Business	16	7.4%	0	14	2	0
Engineering	5	2.3%	0	1	1	0
Math/Statistics	2	0.9%	0	1	0	0
Communications	1	0.5%	0	1	0	0
Design	1	0.5%	0	1	0	0
Economics	1	0.5%	0	1	0	0
Computer Sci. + Math / Stats	1	0.5%	0	1	0	0
Computer Sci. + Eng./Bus.	1	0.5%	0	0	1	0
No major	15	6.9%	12	2	0	0
No response	14	6.5%	1	7	6	0
Low quality response	1	0.5%	0	1	0	0
Total	216	100.0%	13	136	61	1

Note: * Self-identified majors were grouped into common areas of study listed here.

Table 16

Certifications per Manger for Risk Management and/or Cybersecurity

	Interview		Survey	
Number	N	%	N	%
None*	7	31.8	49	22.7
One	4	18.2	87	40.3
Two	2	9.1	69	31.9
Three	2	9.1	10	4.6
Four	3	13.6	0	0.0
Five	1	4.5	1	0.5
Six	2	9.1	0	0.0
Seven+	1	4.5	0	0.0
Total	22	100	216	100

Note: * Includes other and non-certification type responses

Certifications are commonplace in technical professions and, like higher education degrees, can help establish a foundation for knowledge and learning, as well as signal more focused insights into participants' specialized expertise. Many certifying organizations are member-based, such as ISACA or CompTIA, which help establish professional identities and community, as well as further enhance individuals' foundational understanding.

Certification information followed the same data collection and processing as higher education for both interview and survey respondents. Respondents had an open text response option to provide certification details, which resulted in a mix of acronyms and written out names. Table 17 contains frequencies for the reconciled certification names with the certifying organization. I conducted some data cleaning, such as typo correction and recoded non-certification information as none.

Viewing Tables 15 and 16, as expected, most of my interview and survey participants have at least one certificate, with half of the interview and 37% of the survey participants having two or more certificates. Although having five or more certifications was rare among the survey participants, but more prevalent (18%) among interviewees. One interviewee noted having more than 30 certifications but declined to list them individually. Among the 40 listed certifications, CISSP was the most common, held in similar proportion by participants in both groups. Overall, only around 12% of certifications were related to risk management and were not specifically connected to cybersecurity. The most frequent non-cybersecurity specific certification was the PMP, well-regarded within this professional space. The number and diversity of certifications shared demonstrates the wide reach of specialized topics and possibility for more niche communities. However, ISACA and the EC-Council were the most recurring certification organization at 15% and 13% of participants respectively, with $(ISC)^2$ and the Project

Management Institute (PMI) in third place, both at 8%. While all provide sales-based certifications, only EC-Council did not also offer a membership program. Notably, ISACA and (ISC)^2 also develop and share their own framework approaches within their programs, which may influence individuals holding the related certifications to use adopt those approaches in practice. Several other certification organizations, such as CompTIA and SANS Institute, also produce CSRI&A approaches.

Table 17

*Manager Certifications: Risk Management and/or Cybersecurity (Most Frequent)**

Certification	Int. N	Sur. N	Full Certification Name	Certifying Organization
CISSP	10	89	Certified Information Systems Security Professional	(ISC)^2
CISA	2	37	Certified Information Systems Auditor	ISACA
CISM	3	27	Certified Information Security Manager	ISACA
CEH	3	18	Certified Ethical Hacker	EC-Council
CRISC	1	15	Certification in Risk and Information Systems Control	ISACA
Security+	1	15	Security+	CompTIA
CGEIT	1	8	Certified Governance of Enterprise IT	ISACA
CDPSE		8	Certified Data Privacy Solutions Engineer	ISACA
SSCP		8	Systems Security Certified Practitioner	(ISC)^2
GSEC		7	Global Information Assurance Certification (GIAC) Security Essentials	SANS Institute
PMP	3	4	Project Management Professional	Project Management Institute (PMI)

Note: * A full table with all certifications and frequency counts appears in Appendix F

5.1.1.4 External Activity – Active and Relevant Organizations

This subsection directly applies to survey respondents only, as the question about active and relevant organizations came from interview questions regarding where participants obtained new information, but often organizational names were not shared.

Table 18

Number of Active and Relevant Organizations Per Participant

	Active		Relevant	
Orgs	N	%	N	%
0*	61	28.2%	31	14.4%
1	146	67.6%	137	63.4%
2	8	3.7%	37	17.1%
3	0	0%	8	3.7%
4	1	0.5%	2	0.9%
5	0	0%	1	0.5%
Total	216	100%	216	100%

Note: * Includes self-reports of None and missing values

Survey respondents provided their own entries for professional associations in which they are active, such as attending meetings, engaging with other members, or volunteering, and then separately for professional organizations they found relevant. These questions were not mutually exclusive. Most organization submissions were given as acronyms. Due to the common duplication of acronyms, I did not attempt to extrapolate these acronyms to the full organization name, which could introduce some duplication within the reported results.

For the active group of professional organizations, 154 respondents (77%) mentioned 78 unique organizations and nine of those respondents (4.2%) mentioned being active with two or more organizations. This suggests being active with an organization is important to most cybersecurity management professionals; however, activity with only one organization seems typical. Of the 78 organizations, only four organizations were mentioned 10 or more times or had greater than 5% of all organizations as being active, see Tables 18 and 19 for more details.

For the relevant group of professional associations, 185 respondents (83%) mentioned 88 unique organizations and 48 of those respondents (22%) mentioned two or more organizations. It makes sense that participants would report a higher number of relevant organizations than active ones. Despite the higher prevalence of relevant organizations, only five were mentioned 10 or

more times or greater than 5%. Looking at both active and relevant organizations, just under two-thirds of respondents (63%) listed the same organization at least once as being both active and relevant.

Table 19

Top 6 Active and Relevant Organizations

	Active			Relevant		
	Ranked	N	%*	Ranked	N	%*
AEHIS	1	16	10%			
ISACA	2	16	10%	1	32	13%
ISSA	3	13	8%	3	20	10%
$(ISC)^2$	4	10	6%	2	26	8%
CSN	5	8	5%			
ISS				4	14	6%
RIMS				5	10	4%
ISA	6	7	4%	6	8	3%

Note: * Percent from all listed organizations in that group

Information Sharing and Analysis Centers (ISACs) are a subset of interest, shown in Table 20, but only a few participants mentioned them as active and/or relevant organizations, approximately 8% of each group. When they listed ISACs, they almost always listed the same ISAC as being both active and relevant, contributing to similar reporting percentages between groups and in line with similar reporting. Moreover, when viewing alongside their reported critical infrastructure organization, it was not surprising that the reported ISAC was associated with that infrastructure sector. Interestingly, the several ISACs discussed in Subsection 5.1.2.3 below were not reported here as active and/or relevant.

Table 20

Active and Relevant ISAC Organizations

ISAC Code	Active (N)	Relevant (N)	ISAC Infrastructure Sector (Subsector*)
H	2	3	Healthcare & Public Health
ND	2	1	Defense Industrial Base
RE	2	2	Commercial Facilities (Real Estate)
Water	2	2	Water & Wastewater Systems
ACC	1	1	Chemical
EI	1	1	Government Facilities (Election Infrastructure)
MTS	1		Transportation Systems
ONG	1		Energy
REN	1	1	Government Facilities (Educational Facilities)
RH	1	1	Food & Agriculture (Restaurants)
FS		1	Financial Services
Total	14	13	

Note: * Subsectors listed here reflect those available to choose from within the survey.

5.1.1.5 Race, Ethnicity and Gender

Race, ethnicity and gender identity data was collected through the survey, but not asked during interviews (Aspen Tech Policy Hub, 2021).[11,12,13] Response results appear in Tables 20 and 21. The 12 missing data values for each variables come from the same 12 individuals, opting not to provide this data.

Regarding the manager's race and ethnicity, approximately three-quarters of respondents identified as white with most other racial or ethnicity groups ranging between 4-8%. Only one

[11] Initially, I obtained this data based on my observations from interviewees' LinkedIn profile and posts but removed reporting here due to potential measurement bias.

[12] Determining if there were differences among CSR managers by either gender or race and ethnicity in approach use and use selection factors was of initial interest to this study; however, it would likely require the addition of quota or similar sampling strategy and alter the overall direction of this research. It remains an option for future work.

[13] I followed the combined visual reporting format of race and ethnicity values as shown in the Aspen Tech Policy Hub report on Diversity, Ethnicity, and Inclusion in Cybersecurity (2021).

person self-identified as multi-racial or ethnic. Notably, not all the race or ethnicity groups available in the survey appear in the results.[14]

My survey offered multiple response category options for gender to help account for workforce diversity; however, respondents only marked the man and woman groups. This sample included 83% of respondents who identified as a man and 17% as a woman. The female group is underrepresented compared to the 24% women listed in the 2021 cybersecurity diversity study (Aspen Tech Policy Hub, 2021).

Table 21

Manager's Race and Ethnicity

Race / Ethnicity*	N	%
White	152	70.3
Black / African American	16	7.4
South Asian	12	5.6
East Asian	10	4.6
Hispanic / Latino	8	3.7
Southeast Asian	3	1.4
Mid. East / Nor. African	2	0.9
Multiple: White + Hispanic/Latino	1	0.5
Missing	12	5.6
Total	216	100

Note: * Self-identified, multi-choice option, other option provided

[14] There were no responses from the American Indian or Alaska Native group or the Native Hawaiian or Other Pacific Islander group. While this decreases representation for these groups, it should not bias the results overall given these groups are approximately 0.2% and 1.1% of the US population respectively according to the 2020 US Census (Jones et al., 2021).

Table 22

Manager's Gender

Gender*	N	%
Man	169	78.2
Woman	35	16.2
Missing	12	5.6
Total	216	100

Note: * Self-identified, multi-choice option, additional options included: non-binary or transgender, prefer not to respond, and other with text entry

5.1.2 Organizational measures

This subsection provides respondent answers on a series of organizational level questions as additional background information to understand their specific situations.

5.1.2.1 Critical infrastructure sector

This study aimed to span critical infrastructure as broadly scoped by CISA's 16 sectors, established and defined within the US Presidential Policy Directive 21 (White House, 2013). I matched the infrastructure type to CISA's sectors for the interviewees by assessing the description of their companies. This assignment was not mutually exclusive. Organizations from the 22 interviewees coded to 49 sectors, most notably Government Facilities and Information Technology, both with 11 organizations each and were able to capture at least one participant for 11 of the 16 CISA sectors.

The survey listed 34 sector and subsector options, breaking out select subsectors where participants might not be familiar with CISA's groups. For example, Educational Facilities were a subsection for Government Facilities. While survey participants could choose multiple sectors if they applied, none selected more than one sector for their organization. The survey used quotas to prevent an oversample of each of the 34 sectors and subsectors. While none of the quotas

reached the threshold, a side effect of the subsector listing meant aggregating into the parent sectors could potentially have an oversample at the sector level. For instance, Commercial Facilities consisted of Retail, Real Estate, Outdoor Facilities, Lodging Facilities, Gaming Facilities, and Entertainment and Media Facilities. None of them had more than 10 participants each; yet, when aggregated into Commercial Facilities, they summed to 40 participants (18.5%). Additionally, despite efforts to recruit widely, some sectors were difficult to reach, such as Dams or Nuclear Reactors, Materials, and Waste. Nonetheless, these organizations were associated with 15 of the 16 CISA sectors.

Sector breakdowns appear in Table 23 and 24. Given 216 survey participants, an even distribution across sectors would have 13.5 participants on average or a uniform 6.25 percent distribution. Figure 6 shows variance in the mean for each sector with more than twice as many associated organizations for Critical Manufacturing and Commercial Facilities. On the flipside, sectors such as the Dams, Emergency Services, and Nuclear were the least represented sectors. In some cases, the interview data helped shorten or eliminate the survey data's infrastructure gaps, such as with the Defense Industrial Base. Notably, there remain some subsections within the larger, aggregated CISA sectors that do not have any representation, such as the Public Assembly or Sports Leagues Commercial Facilities. Initial assessment posits this gap may affect transferability of this study's findings because when certain sectors are unrepresented, the unique cybersecurity risks, mitigation strategies, and context-specific concerns of those sectors are not reflected in the results, limiting how well findings can be applied to those groups.

Table 23

Survey and Interview Participant Organization Critical Infrastructure Sector and Subsectors

Sector / Subsector	Survey Subsectors N	Survey Subsectors %	Survey CISA 16 N	Survey CISA 16 %	Interview CISA 16 N	Interview CISA 16 %
Chemical	10	4.6	10	4.6	0	0
Commercial Facilities			40	18.5	0	0
Entertainment & Media Facilities	1	0.5				
Gaming Facilities	8	3.7				
Lodging Facilities	9	4.2				
Outdoor Facilities	4	1.9				
Real Estate	9	4.2				
Retail	9	4.2				
Communications			15	6.9	1	2
Terrestrial and Satellite, Wireless, and Wireline Providers, Owners and Operators	7	3.2				
Transmission Providers, Owners and Operators	8	3.7				
Critical Manufacturing			31	14.4	0	0
Electrical equipment, Appliance, and Components	11	5.1				
Machinery	13	6.0				
Primary Metals	3	1.4				
Transportation Equipment	4	1.9				
Damns	2	0.9	2	0.9	1	2
Defense Industrial Base	3	1.4	3	1.4	8	16.3
Emergency Services	1	0.5	1	0.5		
Energy	9	4.2	9	4.2	6	12.2
Financial Services	11	5.1	11	5.1	3	6.1
Food & Agriculture			21	9.7		
Farms	1	0.5				
Manufacture, Process, & Storage	7	3.2				
Restaurants	13	6.0				
Government Facilities			17	7.9	11	22.4
Education Facilities	15	6.9				
Election Infrastructure	1	0.5				
Government Buildings	1	0.5				
Healthcare & Public Health	25	11.6	25	11.6	3	6.4
Information Technology	12	5.6	12	5.6	11	22.4
Nuclear Reactors, Materials, and Waste	0	0	0	0	1	2

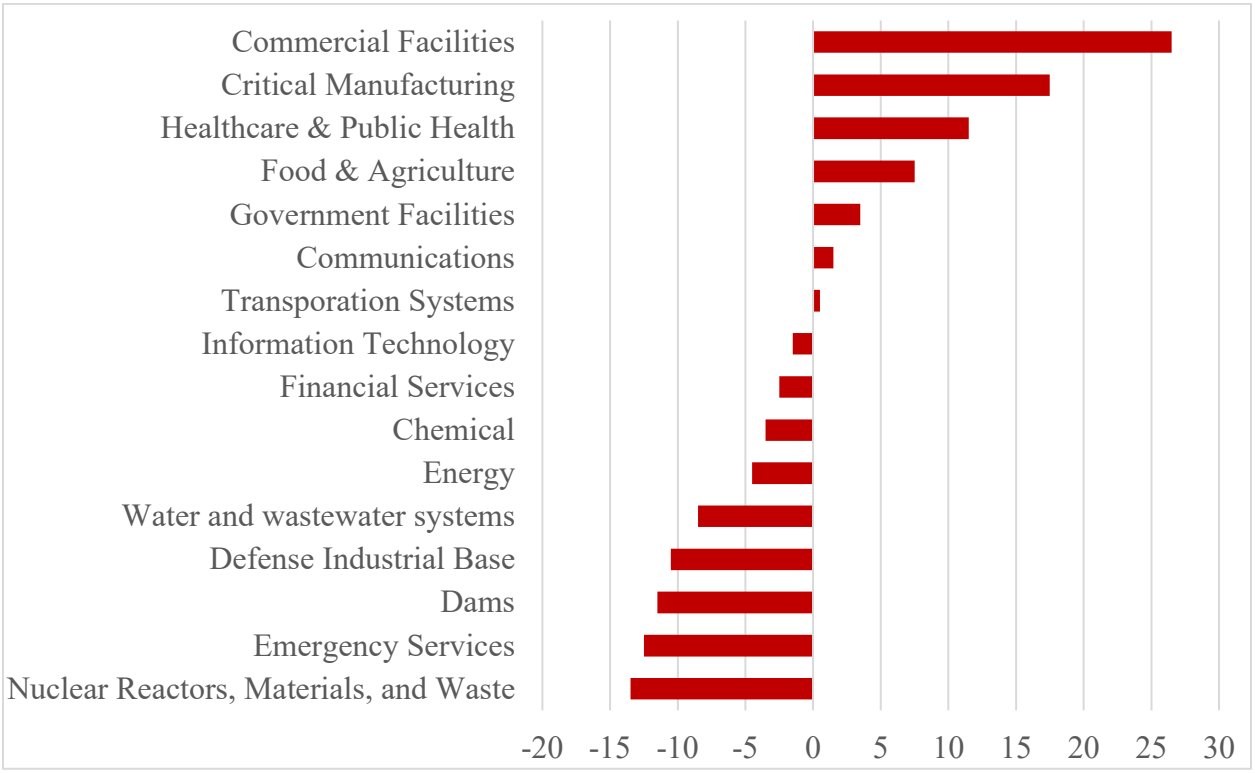
Table 23 continued.

Sector / Subsector	Survey Subsectors N	Survey Subsectors %	Survey CISA 16 N	Survey CISA 16	Interview CISA 16 N	Interview CISA 16 %
Transportation Systems			14	6.5	1	2
Aviation	2	0.9				
Freight Rail	3	1.4				
Highways	1	0.5				
Maritime	2	0.9				
Pipelines	1	0.5				
Post Shipping	2	0.9				
Transit & Rail	3	1.4				
Water and wastewater systems	5	2.3	5	2.3	3	6.1
Total	216	100	216	100	49	100
Number of Sectors*	34		15		11	

Note: * Selection allowed multiple choice and was not mutually exclusive

Figure 6

Frequency Variance from Mean of Participants per Critical Infrastructure Sector



5.1.2.2 Type of Organization and Number of Employees

The respondents represented multiple organization sizes, based on number of employees, in part due to established categories that represented a spectrum of very small to very large organization distributions better than official US government size categories.[15] Likewise, there are a wide variety of organization types represented. Distributions across Tables 24 and 25 differed widely between the interview and survey organization sizes and types, but I did not observe any immediate reasons to suggest these differences would have meaningful impact on the rest of the analysis. Conversely, gaps in interview data here were filled by survey data and vice versa, such as having federal government represented in the interview data but not the survey data as well as state government represented in the survey data but not the interview data.

Table 24

Organization Type by Size based on Number of Employees - Survey Participants

Organization Type by Size (Survey Participants)	< 10	10 - 100	101 - 1,000	1,001 - 10,000	10,001 - 25,000	Missing	Total
Private non-profit organization			6	3			9
Private, for-profit organization		12	97	44	2	4	159
Public, for-profit organization			4	13	5	1	23
Public, non-profit organization			19	2			21
Federal government							0
State government			1	1			2
Local or Tribal government				1			1
Quasi-government				1			1
Total	0	12	127	65	7	5	216

[15] I previously considered using the official firm class sizes established by the US Office of Management and Budget and adopted by other federal agencies such as the Bureau of Labor Statistics; however, the official size groups had nine granular categories that focused on small size firms and the largest group had ceiling of > 1,000 employees.

Table 25

Organization Type by Size based on Number of Employees - Interview Participants

Organization Type by Size (Interview Participant)	< 10	10 - 100	101 - 1,000	1,001 - 10,000	10,001 - 25,000	Missing	Total
Private non-profit organization	1	1	1				3
Private, for-profit organization	5	2	2		1		10
Public, for-profit organization			2		2		4
Public, non-profit organization							0
Federal government		1		1			2
State government							0
Local or Tribal government							0
Quasi-government			2	1			3
Total	6	4	7	2	3	0	22

Among the organization types, as expected, the for-profit organizations far outnumbered the other types with 84% of the survey participants' organizations and 64% of the interviewees' organizations. While most of the organization types are self-explanatory, examples from the data of the quasi-governmental organizations include a municipal water commission and nuclear laboratory.[16] Among the survey data, the public nonprofits are almost entirely identified as part of the Government Educational Facilities or Healthcare and Public Health infrastructure sectors, which aligns well with this organizational type's typically missions to fulfill charity, social services, and other public needs. Looking at the extremely large and small organizations, all but one were for-profit, with the exception being a private, non-profit organization. The entire cluster of organizations with fewer than 10 people from the interview data were private consultants; it is plausible the same holds for the small organization survey results.

[16] Quasi-governmental organizations are often federally funded for- or nonprofit private organizations or government sponsored organizations. See Kosar (2011) for more details.

Table 26

ISAC Memberships per Organization

ISACs	N	%
0	75	34
1	132	61
2	8	3.7
6	1	1.3
Total	216	100

5.1.2.3 ISAC affiliations

Like the individual cybersecurity manager's connection with professional associations, ISAC affiliations can be a source of information and other resources as well as an information-sharing gatekeeper to a network of similar organizations. Interviewee mention of ISAC information was not consistent, and usually in reference to information sharing organizations writ large; therefore, only the survey obtained specific ISAC affiliation data.

Survey participants identified which, if any, ISAC memberships their organizations held. Just over one-third reported not having any such memberships (34%), while organizations had two memberships (3.7%). Twenty of the 26 National Council ISACs were mentioned, and participants added their own ISACs such as Infragard. Altogether, organizations held 154 ISAC memberships across 22 ISACs since selection allowed multiple entries. Refer to Table 26.

The top two listed ISAC memberships included the Health (14.3%) and Retail & Hospitality (11.7%), after which the frequency distribution quickly drops. The ISACs that appeared more than once included Healthcare Ready (n=5), Health (n=4), Information Technology (n=4), Communications (n=2), and Multi-State (n=2).

Table 27

ISAC Memberships

ISAC Memberships	N	%
Health (H-ISAC)	22	14.3
Retail & Hospitality (RH-ISAC)	18	11.7
Communications (NCC)	14	9.1
Information Technology (IT-ISAC)	14	9.1
Research & Educational Network (REN-ISAC)	11	7.1
Financial Services (FS-ISAC)	11	7.1
Automotive (AUTO-ISAC)	9	5.8
Real Estate (RE-ISAC)	8	5.2
American Chemistry Council (ACC-ISAC)	7	4.5
Healthcare Ready	6	3.9
Oil & Natural Gas (ONG-ISAC)	6	3.9
Public Transportation & Over-the-road Bus (PT & OTRB ISAC)	5	3.2
Water (Water-ISAC)	4	2.6
Electricity (E-ISAC)	3	1.9
Maritime Transportation System (MTS-ISAC)	3	1.9
National Defense (ND-ISAC)	3	1.9
Surface Transportation (ST-ISAC)	3	1.9
Aviation (A-ISAC)	2	1.3
Multi-State (MS-ISAC)	2	1.3
Elections Infrastructure (EI-ISAC)	1	0.6
Infragard	1	0.6
Media & Entertainment (ME-ISAC)	1	0.6
Total	154	100.0
Unique ISACs	22	

5.1.2.4 CSRI&A functions

In addition to measures of sector, size, and affiliations, I asked survey participants questions that help unpack a greater understanding of the internal structure and duties within their organization. These distinctions help guide data interpretations in the following chapters.

Table 28

Groups within Organization with CSRI&A as Primary Duties

Group	N	%
IT	188	35.4
Security	146	27.5
Internal Audit	74	14.0
Finance	58	11.0
Separate Risk Management	37	7.0
Insurance	13	2.5
Outsourced	13	2.5
Engineering *	2	0.4
Total	531	100.3**

Note: * Identified as an 'Other' option. ** rounding error

Table 29

Number of Groups within Organization Sharing CSRI&A as Primary Duties

Groups	N	%
1	54	25
2	67	31
3	52	24
4	28	13
5	15	7
Total	216	100

Not only do cybersecurity managers exist within a variety of units within the organization, such as the more traditional IT department, but also units such as security, operations, and compliance and risk. Additionally, their RI&A work is often cross-cutting with other units. Tables 28 and 29 reveal the range of units with whom a cybersecurity manager shares RI&A functions as part of their primary duties. This selection was not mutually exclusive, nor were any guidelines given to qualify the degree of participation for those duties. Only a quarter of organizations keep RI&A duties to a single unit, and just under a third share it between

two units. When shared between two units, Security works with IT around 83% of the time. That percentage decreases when three units share primary RI&A duties, as IT shared with Security, Internal Audits, and Finance 77%, 63%, and 41% of the time respectively.

5.2 Addressing RQ1: What CSRI&A Approaches

In this section, I present findings to the first research question: what approaches do cybersecurity managers use for their RI&A work? These results are descriptive, derived from interview data when participants organically discussed usage or following prompting with examples when they did not. This produced an emergent, initial list of approaches taken naturally from the interviews which I coupled with additional literature to create a multi-choice option list for the survey participants.[17] Selected approaches in the survey then carried over to additional questions discussed here and in the following chapters to discover if those approaches were still in use, opinions about those approaches, and ultimately, why they were selected.

5.2.1 Approaches from Interviews

To better understand which approaches cybersecurity managers use for RI&A of critical infrastructure (RQ1), my interview study asked three questions intending to elicit specific approach names for those currently used, previously used, and suggested for use by third parties such as colleagues or vendors.[18] Approach names could also have appeared organically in response to other interview questions. Individual responses could have contained any number of named approaches and allowed for uncertainty and non-specific answers. Table 30 displays an

---

[17] The approach list used came entirely from the interviewees and is not based on previous scholarship. Consensus building or other forms of filtration of mentioned approaches mentioned is out of scope for this study as it would undermine the primary objective of collecting the approach list, which is to capture authentic, independent, individual perspectives responses.

[18] Interview questions 8, 14, and 15. Additionally, approach names could also appear organically in response to other interview questions.

overview of those named approaches. Most approach names were emergent during the interviews.[19] When prompting approach names, I only mentioned approaches commonly known in the cybersecurity community, such as the NIST RMF or CSF, FAIR, or OCTAVE.

Table 30 shows that cybersecurity managers currently use a wide variety of CSRI&A approaches. Almost 60% of interviewees confirmed using more than one approach; although it is yet unclear if approaches were used simultaneously or at different times or the exact reason why multiple approaches were necessary. More than half of the interviewees (59%) acknowledged using various forms of NIST-related approaches.[20] Numerous industry solutions, such as CIS or FAIR, appear sprinkled across the responses with few gaining any momentum beyond two or three persons per approach. Three respondents stated their organizations use in-house developed approaches that drew from other, more well-established approaches.

Among approaches suggested for use, FAIR featured prominently. FAIR is currently, was suggested, or was once used by nearly 40% of the interviewees but more than half of them mentioned it as a suggested approach to consider. Likewise, 9% of interviewees noted a NIST-based approach was suggested, substantial given this group was already the most popular overall approach in current use with interviewees. Meanwhile, OCTAVE was the specifically named approach most abandoned (13%), followed by a couple instances each of ISACA (generically named) and the ISO 27000 series. Several respondents responded with uncertainty and non-specificity regarding the approaches no longer used or recommended to use, in part for reasons such as newness to their position and lack of historical knowledge.

---

[19] I prompted approach names for approximately half of the interviewees; however, eight of those were probes to determine if more approaches were used in addition to those mentioned organically.
[20] Several interviewees were only counted once for NIST approaches despite some mentioning using multiple NIST special publications, often in combination of NIST with and without specific names, e.g., CSF or 800-53.

Table 30

Number of Approaches Mentioned in Interviews

Approach Types and Comments	Currently Used	Suggested to Use	No Longer Use
AR 25-2 (Army Cybersecurity Regulation)	1		
NERC CIP	1		
NIST 800-30	1		
NIST 800-39	1		
NIST 800-53	4	1	
NIST 800-171	2		
NIST RMF	1		
NIST CSF	9	1	
NIST standards with bits incorporated with portions adopted from various Singaporean CSA & UK GC HQ NCSC approaches	1		
NIST standards (generic)	9		1
Chicago Metrics	1		
CMMC	3	1	
CMMI			1
FedRAMP	1		
DOD centric (unnamed)			1
ISACA (generic)	1		2
ISO 27000 (series)	2		2
ISO 31000			1
ISO non-specific	1		1
Center for Internet Security (CIS/CSC) 18 (20)	3		1
FAIR	3	5	1
MITRE ATT&CK Framework	3		
MORDA			1
OCTAVE	1		3
NetFlow	1		
TOGAF		1	
SOC (1,2,3)	3	1	1
SOC-C	1		
Stoplight charts (red, amber, green)		1	
Endpoint security management products (various)		1	
Tapestry (Dr. Charles Harry)		1	
Cyber Certified Professional (CCP) standards			1
Unnamed process management		3	2
Consultant recommendations	2	8	
In-house solutions	3		1
Unsure	2	1	4
Did not state specific	3	3	2
Used Multiple Approaches (current as of the interview)	13		

5.2.2 Approaches from Surveys

I constructed a list of 26 named approaches, including a combination of NIST special publications, ISO standards, and other commonly referenced models, framework, standards shared from the interviews and found within scholarly literature (e.g., Ani et al., 2019; Landoll, 2011) and industry reviews (e.g., ENISA, 2022). Using that list, I asked survey participants to identify any approaches they ever used at their organization for cybersecurity RI&A processes. Approach use choices appeared as in a single question with multi-select options and included text entry options to allow up to three user-provided approaches.

Every approach listed, except for Tapestry, was selected at least once and three additional approaches were named using the Other entry option, as shown in Table 32. Notably, ISO 21434 was one of the Other entry options and entered by two respondents; this ISO addresses and contains a framework for cybersecurity risk of road vehicles. Not surprising, both respondents also denoted an organizational affiliation with the Auto-ISAC.

Aggregated, participants selected 586 total approaches for an average of 2.71 approaches per cybersecurity manager. Figure 7 shows a distribution of the selected approaches.[21] The most frequently selected approach was ISO 27001 and/or 27002 and chosen by more than half (52%) of survey participants and nearly 20% of all approach selection choices.[22] This two-part international standard offers information security management controls and guidance to implement those controls. The second and third selections are the only others to have more than

[21] I intentionally removed the 28 approach names from Figure 7 to focus attention on the frequencies and the names while also avoiding the challenge of fitting the approach names legibly into the plot.
[22] ISO 27001 and ISO 27002 were companion standards often used together. In 2022, ISO revised them into a single ISO 27002:2022 standard; therefore, I kept them as a single approach on the survey. In my analysis, I combine the names as ISO 27001/2, but listed their full names on the survey to avoid participant confusion.

50 participants choose them with CSC / CIS 18[23] and NIST SP 800-53. Table 31 displays the top seven selected approaches as those which captured at least 10% of all participant selections or 5% of the aggregate approach selection frequency.

Once survey participants selected their approaches from the list, they indicated if they still used that approach or not. If they did, they further informed if that approach met their needs or not. Of the 28 approaches, survey participants rated only 53% as still in use and sufficient.[24] This survey did not delve into reasons for approach abandonment, but I explore possibilities in the next section.

This survey gave consideration for custom approaches for CSRI&A – those approaches that were not conventional, off-the-shelf ready to use approaches that are expected to fit into most organizations. Rather, custom approaches are bespoke amalgamations of other approaches, developed from scratch, or some mixture of the two. By design, bespoke approaches are developed for one or more key reasons which I will explore in the in later sections of this chapter. Six survey participants listed using custom approaches, just under 3% of all participants.

Table 31

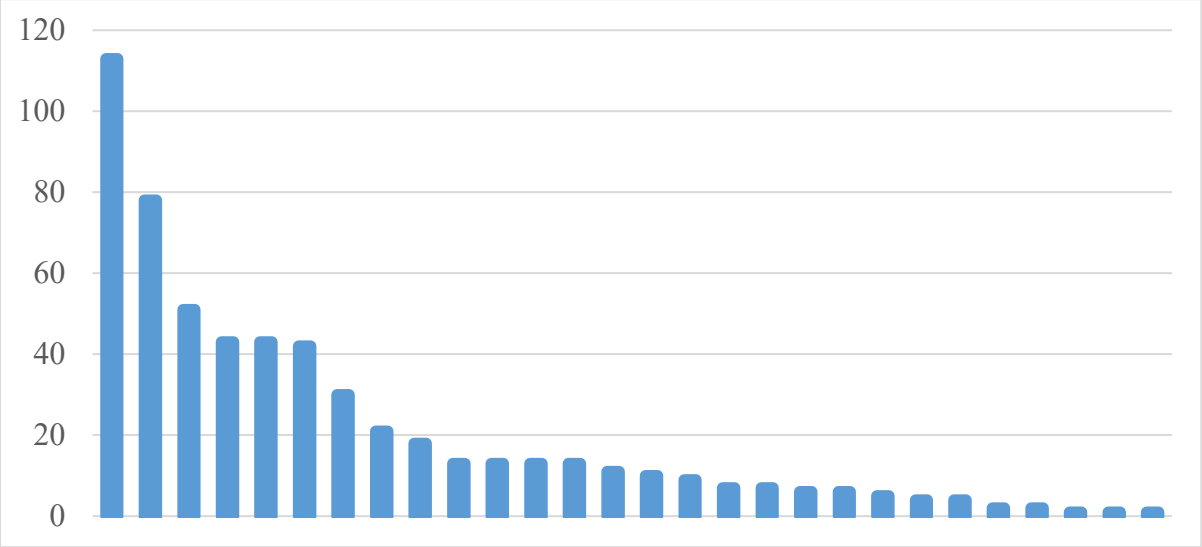
Top 7 Selected Approaches by Survey Respondents

Rank	Approach	N	Total %	Participant %
1	ISO 27001 and/or 27002	113	19.9	52.3
2	CSC / CIS 18	78	13.8	36.1
3	NIST SP 800-53	51	8.99	23.6
4	COBIT	43	7.58	19.9
5	NIST CSF	43	7.58	19.9
6	ISO 27005	42	7.41	19.4
7	MITRE ATT&CK	30	5.29	13.9

[23] The full approach name presented was CIS 18 (or former CIS 20) or Critical Security Controls (CSC) to capture potential name variations.
[24] I required a clear majority here, so ties such as NIST 800-30 with 40% in both Use and Is Sufficient and No Longer Use would not qualify here as a majority despite 20% saying Use but Is Not Sufficient.

Figure 7

*Frequency of Selected Approaches by Survey Respondents**



Note: * X-axis labels removed to focus on visual drop-off. See Table 32 for approach names and frequencies.

Table 32

Survey Participant CSRI&A Approach Selections and Current Use Status

Rank	Approach	N	Sum(N)%	N/216	Do Not Use	Use, Not Sufficient	Use, Yes Sufficient
1	ISO 27001 and/or 27002	113	19.9	52.3	35	30	48
2	CIS 18 (or former CIS 20) or Critical Security Controls (CSC)	78	13.8	36.1	16	5	57
3	NIST SP 800-53	51	9.0	23.6	25	7	19
4	COBIT (Control Objectives for Information Related Technology)	43	7.6	19.9	8	11	24
5	NIST Cybersecurity Framework (CSF)	43	7.6	19.9	5	5	32
6	ISO 27005	42	7.4	19.4	11	5	26
7	MITRE ATT&CK	30	5.3	13.9	12	6	12
8	NIST SP 800-37 Risk Management Framework (RMF)	21	3.7	9.7	1	4	16
9	CMMC (Cybersecurity Maturity Model Certification)	18	3.2	8.3	9	4	5
10	CMMI (Capability Maturity Model Integration)	13	2.3	6.0	3	7	3
11	NIST SP 800-171	13	2.3	6.0	1	3	9
12	PHA (Process Hazard Analysis)	13	2.3	6.0	6	0	7

Table 32 Continued

Rank	Approach	N	Sum(N)%	N/216	Do Not Use	Use, Not Sufficient	Use, Yes Sufficient
13	SCF (Secure Controls Framework)	13	2.3	6.0	3	2	8
14	SOC-C (System and Organization Controls for Cybersecurity)	11	1.9	5.1	5	1	5
15	ISO 31000	10	1.8	4.6	2	0	8
16	NIST SP 800-82	9	1.6	4.2	1	2	5
17	FAIR (Factor Analysis of Information Risk)	7	1.2	3.2	0	3	4
18	NIST SP 800-39	7	1.2	3.2	2	1	3
19	Custom approach (developed in-house and/or with third-party help)	6	1.1	2.8	1	4	1
20	MITRE Shield / MITRE Engage	6	1.1	2.8	4	1	1
21	NIST SP 800-30	5	0.9	2.3	2	1	2
22	NISTIR 8286 (and/or 8286 A-D)	4	0.7	1.9	2	2	0
23	OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation)	4	0.7	1.9	1	2	1
24	ISO 21434[+]	2	0.4	0.9	0	1	1
25	NERC CIP Reliability Standards	2	0.4	0.9	0	0	2
26	IEC 62443 series	1	0.2	0.5	0	1	0
27	Threat analysis and Risk assessment (TARA)[+]	1	0.2	0.5	0	1	0
28	TISAX[+]	1	0.2	0.5	0	0	1

Note: [+] Participant provided approaches through the Other option text entry.

Cybersecurity managers reported using a wide range of CSRI&A approaches for their work, often using multiple approaches. It is necessary to explore the underlying motivations and contextual factors that informed those choices. Understanding what was used provides a descriptive foundation; however, examining why those approaches were selected provides deeper insight into the decision-making processes, organizational influences, and individual preferences that shape cybersecurity practices. The following section addresses these considerations, drawing on participants' reflections and rationales to answer the second research question: why were certain approaches chosen over others?

5.3 Addressing RQ2: Why Those CSRI&A Approaches

Following the discussion about the approaches that cybersecurity managers use for their RI&A needs, this section presents results from interviews and surveys regarding factors that may influence approach selection or, in some cases, abandonment. Understanding which CSRI&A approaches managers of critical infrastructure selected was relatively straightforward. The main contribution here lies in detailed insights into the individual, professional, organizational, and policy practices that shape how and why managers made their approach selections.

As mentioned earlier in this chapter, during the interviews, I asked a wide range of questions covering topics such as how respondents understood RI&A, updated their knowledge, and engaged in CSRI&A processes, along with individual background information. Many of these topics were echoed in the survey, primarily through close-ended questions, and additional topics were introduced based on the initial interview analysis.

This section presents and discusses my analysis in five subsections. I begin with the application of my conceptual framework on approach selection, laying the groundwork for further discussion in the subsequent subsections. The second subsection addresses the role of CSR consultants in critical infrastructure organizations. The third subsection examines the perception and practice of approach choice as influenced by the degree of quantitative measurement features. The fourth subsection compares the differences and overlaps between the selection of NIST and ISO approaches. Finally, I conclude this section with an analysis of findings from association rules related to approach selection.

5.3.1 Framework Analysis of Approach Selection

The three constructs of the conceptual framework—fundamental understanding differences, functional differences, and situational differences—are derived from the literature.

They provide a robust analytical lens for examining CSRI&A approach selection among 216 survey participants and 22 interview participants. Through systematic deductive coding of interview responses and analysis of survey data, clear patterns emerged, revealing where each construct offered explanatory power and where limitations became apparent.

The framework proved useful in capturing the multidimensional nature of approach selection decisions. However, viewing the three constructs as equivalent categories may not fully explain the results, which indicate that cybersecurity managers rarely rely on single-construct reasoning. Instead, they engage in complex decision-making processes that integrate multiple considerations simultaneously. The subsections below suggest that situational differences may not be an independent construct but rather a modifier, and that interactions with situational differences may offer more nuanced insights. Additionally, I will discuss opportunities for future improvement to the framework, including the incorporation of new constructs and a reconsideration of the importance of construct interactions, with subsection 5.3.1.5 illustrating a potential evolution of the framework.

5.3.1.1 Fundamental Understanding Differences: Knowledge and Experience

The fundamental understanding construct showed significant presence in cases where CSR managers relied on their foundational knowledge, professional background, and academic training to select approaches. This construct proved most useful when decisions were driven by the need for shared terminology, common definitions, or alignment with established professional standards. Fundamental understanding manifested most clearly in the selection of widely adopted frameworks like NIST, where managers explicitly valued the common language and established definitions that these approaches provided.

Interviewee 3, a federal government executive, exemplified a counter position where a lack of fundamental understanding could adversely affect approach selection, as illustrated in a discussion about definitions, "I mean, just go to the nist.gov website and type in risk. There's risk for critical infrastructure; there's risk mitigation methodologies. I think, for me, in my journey, it's that you can get lost in a risk discussion" [I3].[25] This reflects how fundamental understanding of risk concepts shaped approach selection by providing clear definitional anchors in a complex field.

Similarly, Participant I3 demonstrated fundamental understanding through reasoning based on professional training, where knowledge is built progressively as one learns:

> So, my class, I have a cartoon that I use that exactly talks to this, and it has two people standing underneath a cliff, pointing up at a rock; that is risk identification. Then it has the two people with the rock still up on the cliff, talking to each other and sharing some papers; that is assessment [I3].

The selection of the approach was informed by insights gained through formal education.

This framework appeared effective in identifying approach selection in transformative educational experiences, particularly in cases where managers had extensive professional backgrounds that influenced their risk management philosophies. For instance, I13's transition from military to civilian cybersecurity demonstrated how fundamental understanding evolved over time, "During my military career, we kept on thinking about insider threat... as my professional career has advanced, we've really kind of changed the narrative from insider threat

[25] I use the following convention to differentiate participant quotes: I for interview participants or S for survey participants followed by an index value to identify that participant within their group.

to insider risk" [I13]. This shift from threat to risk highlights how a manager's foundational knowledge and training impacted their approach evolution and selection decisions.

A private, for-profit telecommunications executive emphasized the importance of common definitions, which stemmed from fundamental understanding, both for the group and individual managers, "We started by determining the scope of the assessment. Everyone involved was familiar with the terminology used in a risk assessment, such as likelihood and impact, so that there is a common understanding of how the risk is framed" [S92]. However, there were instances where fundamental understanding did not perform as expected. In these cases, while fundamental understanding played a significant role in the decision-making process, other influential factors were also evident. For example, a middle manager from a different for-profit, private telecommunications organization noted:

> We had issues with the members from Finance and Insurance not really wanting to participate on defining processes. We had to get all members from the C-Suite together to push those two departments. […] The standard that was followed was the NIST CSF [S196].

In the upcoming subsection 5.3.1.4, I will discuss construct unions and suggest other potential constructs that may provide deeper insights into Participant S196's approach selection situation, where fundamental understanding alone appeared insufficient to ensure consistent approach selection.

5.3.1.2 Functional Differences: Problem-Solving and Performance Optimization

The functional differences construct proved effective in revealing approach selection when cybersecurity managers acted as problem solvers seeking optimal solutions for specific organizational challenges. As anticipated, this construct demonstrated its usefulness in cases

where managers evaluated approaches based on quantifiable performance metrics, resource efficiency, or effectiveness in achieving specific risk management objectives. The framework worked particularly well when managers discussed cost-benefit analyses, implementation complexity, or comparative effectiveness among different approaches.

Participant I2 exemplified functional reasoning in approach selection, where decisions were driven by functional utility:

> We quantify it in terms of dollars, just because it's easy. Everybody understands dollars, and then you can decide whether that is the mitigation worth that how much is the mitigation going to cost? And how much is what's the potential downside in terms of dollars if the risk actually is realized, and then you can make a decision [I2].

The functional construct was especially valuable for understanding approach abandonment patterns, particularly when the approach was cumbersome and resource-intensive. Participant I4's rejection of OCTAVE illustrated clear functional reasoning, "It was very cumbersome. It was very thorough. Very interesting, but it was very, very cumbersome. NIST really started to accelerate. We moved in that direction" [I4]. This choice was based on functional efficiency and reduced complexity rather than theoretical completeness. This pattern repeated across multiple participants who discussed shifting away from comprehensive but unwieldy approaches toward more streamlined alternatives.

Similarly, a food and agriculture executive from a large private firm noted, "Quantify the impact of cyber risks with the likelihood of occurrence, so risk can be managed consistently." This functional choice is common in risk management methods [S202]. Echoed by a telecommunications upper-level manager, "We mostly use quantitative methods, such as cost-benefit analysis," highlighting the role of functional selection in analytical effectiveness [S3].

These responses provide systematic reasoning for functional decisions across various organizational contexts.

The functional construct also revealed important insights regarding resource optimization. A maritime transportation executive discussed tool selection for functional quantification:

> The development of that tool that we use, the risk-based analysis has been very, very helpful. It enlightened a lot of people when you can give them a number. This is how we put it together and help you identify and quantify what these risks are. [I18]

The approach was chosen specifically for its functional ability to quantify and effectively communicate risk to stakeholders.

However, functional differences revealed limitations when managers selected approaches that seemed suboptimal from efficiency or effectiveness perspectives. Some participants opted for more complex, resource-intensive approaches despite acknowledging their inefficiencies. An interviewed upper-level manager in the defense industrial base (DIB) expressed:

> I think that a lot of the frameworks are usually dictated and regulated to you; it stifles a lot of innovative thinking... in the government is because so many of those frameworks are usually dictated and regulated to you [I6].

This underscores how organizational politics and regulatory constraints can override preferences for functional optimization, resulting in potentially suboptimal selections from an efficiency standpoint.

5.3.1.3 Situational Differences: Context-Driven Selection Constraints

The construct of situational differences demonstrated the strongest relationship among the responses, appearing most frequently across interviews and effectively linking selection

patterns that contradicted fundamental knowledge or functional optimization. For instance, selection by government fiat, such as choosing NIST as a federal compliance requirement, illustrates this point. This construct proved invaluable for understanding organizational context, regulatory requirements, and environmental constraints shaped approach selection decisions, regardless of manager preferences or considerations of technical effectiveness.

Regulatory compliance emerged as a dominant situational driver. Participant S206 explicitly stated, “Some of the work we do is mandated by Federal and/or State regulations. This is largely what drives the use of NIST methodologies” [S206]. This represents a clear situational constraint that overrides other considerations. Similarly, healthcare organizations consistently cited HIPAA compliance as a situational driver, with S153 noting, “NIST and HIPAA were followed and implemented. C-suite was in charge with the CISO taking the lead. There was no pushback from the hospital board whatsoever” [S153].

The framework construct proved particularly effective in explaining sector-specific approach selection patterns. Participant I7 illustrated how the banking industry’s context influenced approach selection, “Banks, inherently, are all risk-based. And so, they have to manage risk; no matter what that risk is, they’re used to managing it” [I7]. The situational context of working in banking shaped approach selection based on an established industry risk culture rather than individual preference or technical superiority.

The situational construct also revealed important patterns related to organizational type, size, and maturity. Smaller organizations faced distinct situational constraints that influenced their approach selection differently than larger organizations. For instance, a public water CISO noted that water and wastewater utilities typically have small IT/OT teams relative to the assets and geography they cover, while also facing significant resource constraints to meet compliance

mandates [I20]. Similarly, a cyber education executive with prior experience in critical manufacturing and the food and agriculture sectors highlighted the challenge of adapting approaches for smaller contexts:

> I don't think any organization I've gone into and said, we need to start using FAIR or OCTAVE or whatever. I guess I could see that maybe, if you're looking at vulnerability management and incident response and things, you want to implement attack methodology, and you want to start doing more threat modeling. I could see that as a very tactical thing, but I started with big boxes, and then I start to see how we can get more granular […] but the focus is always going to kind of be on what's important for your company, and where your core competencies lie and in your business value. [I16]

This illustrates how organizational size creates situational constraints that limit approach selection options.

Survey data reinforced these situational patterns across different organizational contexts. A middle manager at a public non-profit educational facility described how post-incident response drove approach selection: "We were not on the same page. PII [personally identifiable information] was obtained during the hack. SOC2 was the standard, and we have the school district's CTO lead the group. The School Board was involved." [S99]. This situational incident response context influenced approach choices, regardless of prior preferences or technical considerations. Interestingly, this participant did not list SOC2 as one of their current or previous approaches in that part of the survey but did indicate having previously used Process Hazard Analysis (PHA) and currently using, and being satisfied with, ISO 27005.

Based on the results thus far, it appears that context always matters. The situational construct proved most effective in unpacking approach selection patterns that otherwise seemed

irrational or suboptimal. When managers selected approaches that contradicted their stated preferences or chose less effective solutions, situational factors were usually present to explain these choices. However, the construct showed limitations in predicting when managers might successfully overcome situational constraints or when they might find creative workarounds that satisfied multiple situational demands simultaneously.

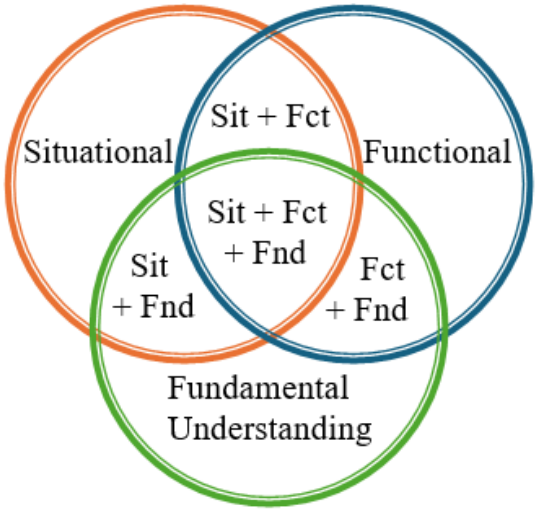
As I will discuss further in the next subsection, situational factors were often involved alongside other construct factors. The difference lies in the fact that responses coded as purely situational were those in which participants focused on their contextual environments. It is logical that such context also existed for participants whose responses were not identified as situational. Each critical infrastructure sector operates within its own distinct environment, shaped by unique pressures and differentiators that demand tailored cybersecurity strategies. However, in cases where the situational construct was not flagged, the context-based factors did not take precedence in the managers' decision-making, making them less relevant to approach selection. Therefore, it matters if the manager actively considers their contextual situation when choosing an approach.

5.3.1.4 Multi-Construct Decision-Making Patterns

The framework's greatest strength emerged in instances where cybersecurity managers engaged in multi-construct decision-making, simultaneously considering fundamental understanding, functional effectiveness, and situational appropriateness. These complex decision patterns revealed sophisticated reasoning processes that single-construct analyses could not capture. The inclusion of multi-construct coding was also valuable for understanding why technically inferior approaches gained widespread adoption and why optimal solutions were sometimes rejected.

Figure 8

Conceptual Framework with Overlapping Constructs



Reflecting on the application of the framework, its constructs can be viewed as building blocks, with different decision processes representing various configurations of the framework components. This shifts the focus from identifying which of the three constructs best applies to the managers shared information to exploring what combination of constructs comprises decision and approach selection. Figure 8 illustrates the framework as a Venn diagram, showing overlapping construct instances in pairs and triplets. Assignment into a single construct or multi-construct portions depends on the actions, values, and other shared thoughts that managers deemed important to their approach decisions.[26]

[26] While the information I deem relevant to approach selection and the constructs into which I code that information may differ if I were to directly observe the CSR managers, I suspect that I would still observe instances of multi-construct decision processes based on the findings thus far.

5.3.1.4.1 Evidence of Multi-Dimensional Reasoning

Participant I7, a risk manager in the financial sector, initially discussed content that leaned heavily toward one construct but later shifted ideas that aligned with other constructs. Portions of my conversation with Participant I7, shared here, demonstrate decision-making content that spans all three constructs. Previously, I shared insights from Participant I7 about the situational context surrounding the banking sector's risk culture. Participant I7 further reinforced this situational view:

> Banks are a little bit risk averse, in a good way. You don't see banks out there taking unnecessary risks, no matter what it is. So, they will be very deliberate in their decision-making and ensure that they have the data to back up that decision. [I7].

Later in the conversation, a fundamental understanding emerged when I7 emphasized the importance of shared language and definitions among risk assessment teams:

> Teams that are doing some of the process-level assessments do not necessarily have a heavy technology background. That's where the experts who own the process can go and say, I own the asset and that's not the risk; the risk is this. [I7].

This highlights essential concerns regarding common terminology and shared understanding, which were further compounded by the banking sector context when Participant I7 discussed cyber qualifications specific to the industry:

> The Federal Reserve does what they call cyber horizontal exam. They'll look at all the banks, at the same time, essentially, or pretty close together. They're looking at the same things for all the banks. So, it kind of gives them a baseline across the banks, and that's a big deal. [I7].

Elsewhere in the interview, Participant I7's thoughts shifted to functional reasoning based on quantitative preferences tied to performance effectiveness, "It's more qualitative or quantitative now... it's got more metrics, you know, driven. And that's a good thing... I think it needs to be underpinned by the quantitative data" [I7]. This illustrates a functional evaluation of capability and measurement effectiveness.

Finally, Participant I7 brought all three constructs together when discussing global cyber operations efforts to enhance their risk assessment:

> A key challenge in a large organization is maintaining consistency when different groups perform similar assessments. […] We want to make sure that we're standardized as much as possible, and sometimes having different groups performing different assessments, there was a little bit of a lack of standardization last year on some of them. Take identification of the likelihood, an impact from something happening. You can go what's the impact, and you have some people go well, the impact is the sky is falling, and others go, it's really not that big of a deal. […] One says impact is really bad, because if it goes wrong, the regulators are going to close the bank. The other one is like, now things go wrong, but we still had these other things in place to handle it. Also, one of the things that helps us is the quantitative metric piece. That is, here's the data that underpins that it [which] goes a long way to eliminating that subjectivity because all models are wrong, some are useful. You can't just take the metric and go, this is absolutely it and then not apply any sort of gut feel or the knowledge that you have from your experience, but that quantitative metric helps eliminate that subjectiveness from the discussion. [I7]

In this part of the interview, I7 connects functional efforts through core quantitative metrics related to likelihood and impact, alongside standardization efforts. These are necessary

functional choices to eliminate organizational subjectivity and create a reliable baseline for comparison across risks and teams. At the same time, Participant I7 addresses the fundamental understanding of how groups interpret assessments and the standardized results, highlighting inconsistencies in risk perception and subjective judgments. Participant I7 integrates both functional and fundamental understanding within the situational context, considering the influence of regulators and the fears among some groups regarding potential bank closures based on assessment results.

Similarly, a senior director exhibited multi-construct decision-making throughout the interview, drawing on experience from both the IT and DIB infrastructure sectors. Fundamental preferences emerged in valuing shared understanding in decision-making, "I like quantitative because it is the one that will make the most sense to a decision maker" [I22]. Functional selection based on decision-making effectiveness was evident in statements like, "if I can walk in with a quantitative analysis of risks, here is what we believe the cost will be [...] that right there is compelling, and that will get you the resources you need" [I22]. Situational constraints from organizational procurement rules were highlighted in comments such as, "the government procurement is different than commercial procurement [...] Why are we using Microsoft Office, or office 365? Right now, I didn't go out and pick it" [I22].

5.3.1.4.2 Framework Interactions, Construct Tensions, and Refinement

The framework revealed important interactions between constructs that single-construct analyses overlooked. In many cases, constructs operated in tension, creating complex decision trade-offs. Managers frequently encountered situations where functional effectiveness conflicted with situational constraints or where fundamental understanding supported approaches that situational factors rendered impossible to implement.

An upper-level manager of a private IT firm illustrated these construct tensions in consulting contexts. From a functional perspective, the manager noted, “If I don’t have enough time to do a thorough one, like I want to, if I don’t have enough manpower to effectively do it totally 100%” [I11]. However, situational demands created different pressures, as illustrated by a mock conversation the manager shared with a client, “If I show up as [COMPANY NAME], and someone goes, yeah, but can you assess me on NIST? I go, sure. Is that the one that makes the money come out? Yeah, for you. Good.” [I11]. This demonstrates how situational revenue constraints override functional optimization preferences.

The framework also revealed how constructs could positively reinforce each other. When fundamental understanding aligned with functional effectiveness and situational appropriateness, selecting an approach became relatively straightforward and sustainable. A former senior cyber director from an accounting firm turned CSR educator described such alignment, “So somebody pointed me to that that was one of those places, and it was that document very specifically. And if our clients get breached, we’ve got to be able to demonstrate, realistically, that what they’re doing is reasonable” [I15]. Here, fundamental knowledge of industry standards (CIS framework) aligned with functional adequacy for demonstrating reasonable security and situational legal requirements for due diligence.

5.3.1.4.3 Framework Limitations and Areas Where Single Constructs Proved Insufficient

Despite the framework’s overall effectiveness, several areas emerged where the three constructs fell short in explaining the influences on approach selection decisions. These limitations provided important insights into the boundaries of the framework and suggested areas for potential refinement or extension.

While situational differences encompassed organizational context and constraints, some political factors operated at interpersonal levels that the framework did not adequately address. Alluding to these dynamics when discussing a virtual CISO position and drawing from extensive experience across several critical infrastructure sectors, I16 stated, “There’s really no authority[when] you are still seen as a consultant, but [when] you’re an executive advisor, you have had the experience of doing many things and holding high level positions over many years” [I16]. The framework’s constructs could explain the situational constraints of consultant status but struggled with the subtle authority and credibility dynamics that influenced which recommendations were accepted or rejected. Thus, the framework may struggle to fully capture the political dynamics and power relationships that influence approach selection and fall outside the traditional situational construct.

Similarly, some participants described approach selection decisions that seemed to reflect personal preferences or individual personalities alongside their professional judgment based on fundamental understanding, functional effectiveness, or situational appropriateness. These individual psychological factors operated outside the framework’s scope but clearly influenced selection patterns in some cases. A VP executive, when asked about CEO preferences, mentioned:

> Our new CEO likes to use a safer matrix. It’s three by three, and I’m like, this is bad. I think you should do this. And he was like, okay, I’ll give you a little bit. We’re gonna use matrices properly, or better. And he was like, okay fine. [I17]

Likewise, a water utility director discussed the tension between organizational and personal preferences, “Sometimes the informed versus the uninformed, there tends to be a tension until we

educate people about why we do it this way versus why we do it, and why you think we should do it this way." [I19]

The framework also offered limited insight into how approach selection patterns changed over time as managers gained experience or as organizational contexts evolved. While individual interviews captured snapshots of current reasoning, the framework did not adequately address learning curves, adaptation processes, or the evolution of selection criteria over extended periods. An IT sector senior director reflected on how major external events forced organizational adaptation and drove a shift toward proactive risk assessment as a necessity for professional survival:

> Previously in cybersecurity, it was all reactive. It was all, we've been hacked or the guy down the street was hacked; we better do something. I would mark this shift, starting in 2017, after the Equifax hack, where people are like, I need to be forward-thinking, or else I'm out of a job. Or, so that if something did happen, I at least have evidence to show, look, I was doing something, we were doing something. [Referring back to previously mentioned pen tests,] these types of risk assessments are more effective communication tools to higher-level executives and boards. […] You're also seeing it become a bigger requirement with insurance policies as well. Insurance policies are requiring organizations to do something pretty proactive. Because someone who thinks about security inherently is 99.99999% more secure than someone who's never thought of it at all. [I11]

The framework could explain the current fundamental understanding or functional rationale but provided limited insight into the evolving process of those constructs and how that evolution influenced approach selection over time. However, it remains unclear whether some of the

approaches also reflect changes over time, as the participant did not mention any shifts in approach based on changes in fundamental understanding or functional perspectives.

Additionally, the framework relied heavily on post-hoc rationalization, as I did not observe participants making their approach selections in real time; instead, I discussed decisions they made in the past or might make in the future. While participants articulated many factors influencing their choices—including trust, experience, and organizational context—the semi-structured interview format may have encouraged them to reconstruct their reasoning in ways that seem more deliberate or logical than the actual, often intuitive process. For example, one participant with multi-sector leadership experience reflected, "A lot of what I do is based on what has worked before, but I probably couldn't map out every step if you asked me to" [I16]. Another senior manager from the maritime transportation sector noted, "You kind of just know when something fits your environment, even if you can't always explain why" [I18]. As a result, some subtleties of tacit knowledge and professional intuition may not be fully captured, suggesting that the real-time selection process is more experiential and context-dependent than the framework constructs alone can explain.

While the current framework excelled at identifying patterns in approach selection in many cases, there are numerous instances in which the findings were less clear among the constructs. Future work can explore variations of the framework, perhaps expanding to consider other areas of interest in approach selection, as discussed below.

5.3.1.5 Evolving the Conceptual Framework

This study served as an initial proving ground to assess this framework's applicability using interview and survey participants. Its use is descriptive and explanatory, but not predictive. The framework worked well as a discussion aid when mapping participants' responses regarding

their approach selection processes and outcomes. However, the framework fell short in mapping all response evidence to mutually exclusive constructs. Instead, some instances were mapped to two or all three constructs, indicating that there may be additional construct dimensions. Furthermore, beyond the evidence already coded as situational, most CSR managers included background details—such as critical infrastructure needs, internal or regulatory policy environments, and influence from other individuals or groups—that were not always explicitly discussed as reasons for selecting an approach. More time and probing might have uncovered details suggesting that those decisions should also be mapped as situational.

With a potential overabundance of situational findings, it is plausible that future considerations of the framework may view situational factors as a horizontal construct that spans both functional and fundamental dimensions, rather than as a separate individual pillar. Figure 9 below illustrates the current framework on the left, with all three constructs represented as equal pillars, and a revised version on the right. Notably, the revised framework introduces a new construct that is not tied to a specific theme and serves only as a visual aid. Future iterations of the framework could incorporate one or more additional constructs based on arguments for those thematic dimensions. Figure 10 shifts the perspective to consider the constructs as not mutually exclusive, replacing the situational component with one or more new constructs, such as political influence. Additionally, Figure 10 positions the situational construct within an encompassing orbit around all other constructs, echoing the discussion in subsection 5.3.1.3, which emphasizes the importance of context. Visually, the dashed line representing situational factors indicates that, although situational context is ever-present, it is not always acknowledged; the extent to which a manager references situational factors correlates with their relevance in the approach selection process.

Figure 9

Current and Potential Future Conceptual Framework Designs

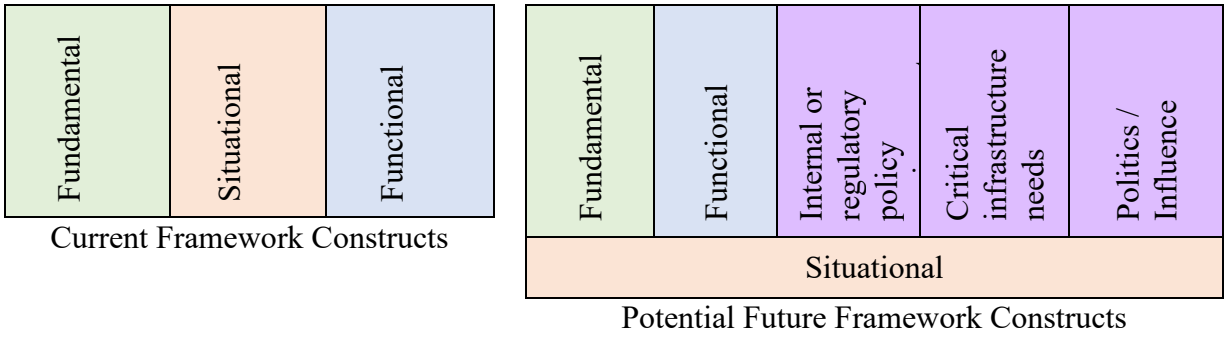
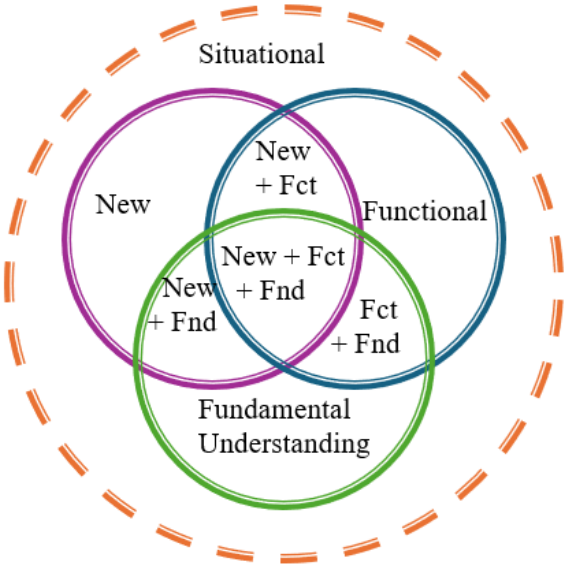


Figure 10

Potential Future Conceptual Framework with Multi-Construct Design



Based on the results thus far, it appears that context is always significant. The situational construct has proven most effective in unpacking approach selection patterns that may otherwise seem irrational or suboptimal. When managers selected approaches that contradicted their stated preferences or opted for less effective solutions, situational factors were typically present to help explain these choices. However, the construct has limitations in predicting when managers might

successfully navigate situational constraints or when they might devise creative workarounds that address multiple situational demands simultaneously.

As I will discuss further in the next subsection, situational factors often interact with other constructs. The key distinction is that responses coded as purely situational were those in which participants concentrated on their contextual environments. It is logical that such context also existed for participants whose responses were not identified as situational. Each critical infrastructure sector operates within its own distinct environment, shaped by unique pressures and differentiators that require tailored cybersecurity strategies. However, in cases where the situational construct was not flagged, it became evident that context-based factors were not at the forefront of the managers' decision-making, making them less relevant to approach selection. Therefore, it is important for managers to actively consider their contextual situation when choosing an approach.

5.3.2 Role of External Consultants

Decision-making to adopt CSRI&A approaches was often made in consultation with third parties. Although how managers leveraged those consultants varied widely. These differences may have substantial implications for not only cybersecurity decision-making, but other organizational behaviors. External consultation occurred when the organization gained value from actors outside the organization, typically in a formal contractor-client relationship. It can also come informally through the manager's networks and other professional circles, such as the ISACs and professional cyber associations; however, the data was mixed on how participants referred to network-type contacts as either being closer to external, if the relationship was more like an informal consultation [I21] or treated like an extended work colleague [I5]. Some organizations have formal internal consultant roles and job positions, and the survey question did

not adequately distinguish between an internal consultant and an internal consultation that could be just a water cooler chat with a colleague. Therefore, to avoid potential misrepresentations of the survey data, this subsection focuses on findings from external consulting.

Of the 216 managers surveyed, approximately one-third reported some form of external consultation. While 32% is not a majority, it is not trivial either. As to why so many organizations use external consultants, one interviewed chief executive in the education and communications sector [I1] noted that "everyone has an opportunity to learn" when referencing the advantage of fresh, outside perspectives, and that it is a part of tapping into "dependency of the task with multiple streams in constant communication and continuous improvement." An interviewed director in the financial sector [I15] described incorporating consultants as being important for a "feedback loop." They also mentioned how external advisors can influence "management culture and change leadership" [I15].

Some situations called for external consultants to work with other outside consultants which can add complexity layers for approach development and selection. Interviewee 10 reflected on an occasional necessity to "work with a couple of trusted third-party partners that solely focus on critical infrastructure." They exchanged views with each other and the CSR manager on evolving trends and tools. Their engagement promotes knowledge sharing within the broader information security environment, as well as promotes diffusion of various approaches. Other times, external consultants worked in a nested relationship, with a subcontracting consultant being administratively one step away from the CSR manager. Such situations typically occurred when a subcontracting consultant had necessary expertise like with HIPPA compliance [I10; I17] or financial reporting requirements [I15].

I found three core topic areas where support from external consultants could affect a CSR manager's approach selection: decision confidence; regulatory and legal compliance; and strategy, operations, and resilience. These areas are not mutually exclusive, and do not have to be as the same consultant may perform one or more of these functions for the manager or their organization. Such consultants often act as boundary spanners between individuals across central business functions.

5.3.2.1 Consultants for Decision Confidence

When it comes to decision confidence, CSR managers rely heavily on external consultants to bring defensibility, independence, and clarity to their approach selection and results. Consultants provide validation for chosen frameworks, offer impartial assessments, and are instrumental in creating outputs that withstand scrutiny at the board or executive level. As one participant noted:

> Cost-benefit analysis is a crucial aspect of our cybersecurity standard evaluation process, where we consider resource consumption and applicability of the standards in our specific situation and it is conducted mostly by higher management with the help of hired external consultants (from the big advisory companies [S52].

Another highlighted, "Before we make any decision, we always consult with external cybersecurity experts and run an analysis to make sure it's beneficial for us." [S56]

External consultants also bring benchmark insights and ensure rigor in both analysis and communication. Managers described processes in which "we review recommendations, consult with outside experts and send for approval to cyber security and finance dept." [S9] and "With the help of external consultants we do the analysis of the cybersecurity risks and then we make a conjoint decision based on various factors, cost, necessity etc. We hire external consultants in

order to get a different view of our problem and choose the best solution." [S67] This external lens is especially critical when companies have less experience or face disagreement internally: "Since we don't have a lot of experience as a company with this, we tend to contract advisors who basically do most of the hard work, and we have some of the people from these companies on retainer. They however do consult with our higher management and it's normally a joint decision on which standard we are to adopt." [S65]

Finally, board-ready, credible outputs depend on the independent assessment and strategic recommendations provided by external advisors—which build collective confidence in the approaches taken. As reflected by managers in commercial facilities and government facilities sectors respectively, "our thought process really just started with what all we need to do to ensure our infrastructure was secure. It made the most sense for us to use vendors and in-house decision makers to figure out the best approach." [S89], and "Based on various factors such as cost, necessity, and effectiveness, we make a joint decision with our external consultants." [S164] These insights show that independence and credible data are central to the consultant's value for CSR managers seeking to justify decisions and recommendations throughout the organization.

Despite the many instances of expressed value of external consultants providing decision support, it is worth mentioning that not everyone in an organization equally agrees with or is ready to have the external consultant participate. Many of the interviewees recognized the decision-aid value of external consultants, having served as both executives who hired the consultants and periodically as consultants for other organizations. Participant I3 shared a constant challenge, "working with other business units, colleagues, managers, executives to convince them that the thing that you're elevating and discussing is important, that it's real."

Similarly, Participant I5 touched on the wider reach of other decision-makers within these groups that affect information dynamics, and by extension which approaches could be used and to what extent, “the cybersecurity people aren’t the ones to do that. It’s actually the mission owner, the people doing the mission, who are the ones who can say with a level of trust, this is what would be the impact,” and that effective assessment requires “all the key players in the room.” [I5]

Yet, this is complicated when those involved may not share the same cyber or risk lexicon. A key challenge in this group space is the varied understanding of “risk,” with interviewees noting that “you get 10 people, they’re going to tell you 10 different things. And then you’re going to try to make sense of that” [I1], while there is also a clear need for a “common list of terms” within the field [I5]. The wider view consultants take helps them level set language and communication. “People identify risk differently, depending on what their job roles are, and what their sectors are,” [I10] while consultants help with “acknowledging the distinct but interconnected nature of these environments” [I20].

In such situations, consultants play a vital role in linking groups within organizations, including those with broader decision authority. An external consultant can be seen as a more neutral source, even an arbiter, for groups under tension. Managerial testimony revealed the depth and successful work of consultants. Organizations often bring in consultants as a “go between for the school leadership, technical team, school board and other advisory groups,” with consultants informing them of “similar issues and solutions used in other localities” [S9]. Consultants are essential to “achieving alignment through an ‘interactive process with staff involved in decision-making’ “ [S5]. Furthermore, consultants used a “nominal group technique to foster understanding [of] risks, both operational and financial” to build consensus [S38].

External consultants not only enhance decision confidence for CSR managers, but they also play a key role in helping organizations meet evolving regulatory and compliance demands. As compliance requirements grow more complex, external experts provide authoritative guidance to align cybersecurity practices with legal and industry standards.

5.3.2.2 Consultants for Regulatory and Legal Compliance

External consultants play a pivotal role in supporting CSR managers as they navigate regulatory and legal compliance situations. These experts help organizations interpret the sometimes-ambiguous language of regulations, benchmark against industry standards, and translate statutory requirements into operational practices. One participant described, “Once we understand our needs when it comes to cybersecurity and the legal requirements, we evaluate the standards with the help of an advisory company and then go into implementation” [S34]. This external perspective ensures both accuracy and practicality in approach selection, particularly when internal expertise is limited or regulations are newly introduced.

Several organizations emphasize the consultant’s ability to harmonize internal processes with complex compliance environments. As one participant shared, “We seek external cybersecurity experts to determine the necessary resources and start implementing the selected standard after identifying our needs and regulatory requirements” [S50]. Another emphasized how external advice is built into the decision workflow, “We first understand our cybersecurity needs and regulatory requirements, on a C level, and then work with an advisory company that we hired to evaluate available standards before proceeding with implementation” [S51]. Consultants also facilitate high-level compliance decisions, such as when “C-Suite and advisory board met to help deliver new compliance workflows and it was at that time we decided an outside consultancy was needed to determine final standards” [S81].

In regulated sectors, third-party validation is especially crucial. “It’s important to know are there any regulatory requirements that we have to follow and after we see which standard is most relevant for our case as make a selection in consultation with internal stakeholders as well as hired external consultants” [S55]. Some organizations went further, outsourcing significant compliance tasks to consultants to “ensure we hit compliance and regulations within our industry” [S105] and “help ensure the process went smoothly” [S105] when adopting standards like CIS 18 and PHA for the chemical sector and ISO 27001/2 for commercial facilities respectively.

In the healthcare sector, HIPPA was commonly referenced alongside CSRI&A activity as part of the approach selection process. For instance, consultants work alongside C-suite officers to “bridge the gaps of patient information data collection” [S178] required under HIPAA or “met the HIPPA compliance timelines” [S201]. Large consulting firms like Grant Thorton [S119], Boston Consulting Group [S143], and McKinsey [S173] were often part of response after a cyber breach and subsequent recovery. In some cases, the consultants also helped the organization match the CSRI&A approaches to the HIPPA compliance work. One upper-level manager shared, “NIST standards and HIPPA are mandatory,” and that, “gaps in security controls were identified by outside consultants” [S145]; notably, this manager also reported using the NIST RMF and CSF after abandoning CIS 18. Another manager shared the value of consultants helping with “HIPPA in conjunction with ISO to help provide end-to-end governance” [S173].

Taken together, these insights illustrate that consultants are not just facilitators, but are often essential partners in the compliance journey, blending legal understanding, operational expertise, and objective assurance for CSR managers who must confidently choose, implement,

and justify their organization's cybersecurity approaches. Moving from compliance to daily practice, consultants are also essential in translating these requirements into operational processes that strengthen organizational resilience.

5.3.2.3 Consultants for Strategy, Operations, and Resilience

External consultants are often key partners in strengthening strategy, operations, and operational resilience as CSR managers select and implement their CSRI&A approaches. These consultants provide an objective, outside perspective that bridges internal gaps to support programs that span technical and governance domains. For example, a manager who reported using four different approaches shared:

> The cybersecurity programs including corporate governance, notification and reporting requirements, and asset management and security have been an exhausting process that our C-Suite team and Board have been involved with. Use of consultants (financial and risk) were part of the process [S32].[27]

Collaboration with consultants helped align executive, IT, and plant operations teams in the development and implementation of security frameworks, creating a unified approach, as when, "[an] executive team worked with the IT team and with the plant operations group. Fortunately, we were on the same page with the help of a risk consulting firm" [S189].

In smaller organizations, consultants lend both industry-specific insight and practical solutions. "They assisted in providing us a few options, including costs and time, which our CIO then decided what would be best. The consultants knew our industry and what we needed to accomplish to ensure we were doing everything we could against threats," shared a middle

[27] This upper-level manager in the communications sector reported currently use of CIS 18 and NIST CSF as sufficient, current of COBIT but that it is insufficient for use, and previously used ISO 27005.

manager of a food and agriculture sector organization with fewer than 1,000 employees [S192]. These examples illustrate how external support not only brings clarity and objectivity but also directly supports the strategic alignment of cybersecurity processes with organizational culture and mission.

When faced with complex incidents or the need for rapid response, consultants help organizations prioritize vendors and implementation plans—such as after "raids on our cloud services. [The] CISO and CTO were involved to lay out implementation plan [and] utilized an external consultant to help prioritize and select vendors" [S131]. For many firms, the practical challenge of covering all operational risks leads to deep reliance on external partners: "we rely on a third party for the risk identification and then our cyber security team executes" [S30], and "we have found that using third parties is the best way to ensure areas of cybersecurity risk are not overlooked" [S31].[28]

Consultants' operational impact often extends into embedded support and execution. "Our company has outsourced pretty much all of this to third-party vendors but have enough knowledge to know what basic coverage we need and take the advice of our vendors for the rest" [S87]. Others describe sending process layout tasks or even full implementation to vendors, such as when one manager "notified our outside vendor to help us layout our processes. We had the entire executive team work on a specific task force team" [S82], and another "outsourced the recommendations to a vendor who also helped us implement it as well. That was a C-Suite decision" [S107]. Additionally, consultants may embed directly with internal teams or lead

[28] For the operationally curious, in these cases, the rapid response consultant support led to varied approach choices, with COBIT and ISO 27001/12 used after the cloud service raid on a food and agriculture organization [S131] and the others used ISO 27005 for a critical manufacturing organization [S30], and NIST SP 800-53 for a financial services organization [S31].

arduous transformation efforts, as happened with a manager's use of ISO 27001/2, "our consultant group really spear headed the need for this and guided us through the implementation process" [S126].

Using consultants for operational support helps CSR management of people, finance, and other resources. It allows the cybersecurity teams and leadership to focus on strategic issues while partners provide expertise and manpower for tasks like risk assessment, process improvement. A manager mentioned this was the case with ISO 27005 after they "considered the input from our IT team and then outsourced the heavy lifting to an expert vendor. The two work alongside each other to ensure our risk identification approach is the best" [S137] , and similarly another one with ISO 31000 when shifting operational priorities, "we wanted our team to focus on other more important internal matters so we decided the best approach would be to outsource" [S156]. Others made the financial case since consultants can be used on a schedule or ad hoc, unlike a regular employee, as echoed by a manager that "tend[ed] to rely on external advisors who do most of the hard work, and we have some of them on retainer" [S161]. In each of these cases, external consultants enhance operational agility and help organizations build cyber resilience into their everyday activities.

As organizations build partnerships with external consultants to guide CSRI&A decisions, it becomes clear that the process of selecting and implementing RI&A approaches is deeply influenced by how outcomes are measured and reported. In the next section, I discuss preferences for qualitative versus quantitative measurement, which relatedly can drive not only the kind of evidence consultants provide, but also how results are interpreted by leadership and regulators. Understanding these measurement preferences is critical, as they shape both the perceived effectiveness and strategic alignment of cybersecurity initiatives.

5.3.3 Qualitative and Quantitative Preferences and Why It Matters

The following section explores how study participants expressed qualitative and quantitative preferences in their approach to cybersecurity risk measurement and why these preferences have practical significance for CSRI&A outcomes. Building on insights from the preceding discussion of external consultants, the six subsections featured here evaluate different facets of measurement choice and justification. The review then transitions to an examination of how managers navigate compatibility and conflict among competing risk identification and assessment approaches, before turning to association rules.

5.3.3.1 Division in Expressed Preferences

> Measuring the cyber risk present at an organization is nontrivial, and when you set the requirement of delivering on quantitative measurements rather than subjective and qualitative measurements, it becomes almost beyond daunting (Hubbard & Seiersen, 2016, p. xii).

Exposure to new ideas or familiar methods can motivate CSR managers to (re-)examine their preferences and capabilities. Within this context, the tension between qualitative and quantitative approaches becomes particularly significant. CSR managers must weigh the merits of each method while also considering how recommendations align with their organization's culture, reporting needs, and resource constraints. Consequently, preferences for qualitative versus quantitative methods, and the ways in which these are integrated, are not merely abstract academic debates but critical choices that influence how executives understand, prioritize, and respond to cybersecurity risk.

According to interviewees, quantitative measures of CSRI&A are regarded as the gold standard. Interview and survey statements highlighted essential attributes often associated with

quantitative measurement-based choices: reasonableness, consistency, and precision. One CIO from a large quasi-governmental organization spanning the energy and water sectors described how precise quantitative data metrics provide a "level of precision that gives you comfort that it is reasonable, and it is a consistent method across all of your risks" [I19]. More than a quarter of interviewees expressed support for quantitative risk measures. For some, quantitatively assessed risk is deeply ingrained in their industry, as reflected by the Director of a large public for-profit financial sector organization, "[banks] have to manage risk, no matter what that risk is; they're used to managing it, and the banks are very data-driven" [I7]. Similarly, around 22% of survey respondents echoed such preferences in their open-text responses regarding their approach selection, using terms like cost-benefit analysis assessment, a desire to quantify impact, ascribing a financial value, or the cost of implementation. For instance, one upper-level manager at a medium-sized private for-profit communications organization plainly stated, "we mostly use quantitative methods, such as cost-benefit analysis" [S3]. Additionally, an executive manager at a medium-sized private for-profit organization in the restaurant sector noted they, "quantify the impact of cyber risks with the likelihood of occurrence so risk can be managed consistently" [S202].

Given this strong perception that quantitative measures represent the ideal, I next sought to understand which measurement types resonate with managers in practice. Survey participants were asked to identify their RI&A measurement preference and were provided with three response options: explicit numeric values representing more quantitative measures; assigned numeric scales or percentages; and descriptive scales. The latter two are ordinal scales that serve as proxies for quantitative measures, favoring a qualitative rank-ordered context often found in

risk matrices. All three are common ways to measure risk (Hubbard & Seiersen, 2016) and should thus be readily understood by most cybersecurity risk managers.

Yet, interest in fully quantitative measurement is not so clear. Increasingly precise levels of measurement can reduce potential uncertainty in the items they assess—such as numeric ratios over ordinal scales and both are generally better than heuristics alone (Hubbard & Seiersen, 2016). Despite this purported superiority, the field of cybersecurity risk analysis remains strongly influenced by managerial perceptions driven by heuristics, as experiential estimates often inform the determination of ordinal scale measures (Taylor, 2015).[29]

When surveyed about their measurement preferences, cybersecurity managers reported that strict quantitative measures were the least preferred option. Figure 11 shows that only 15% of respondents favored explicit numeric values, a significant decrease from those who expressed a preference for using quantitative measures. This disconnect may be explained by the remaining two options. Four times as many respondents preferred assigning numeric scales or percentages over explicit numeric values, while 25% favored descriptive scales. The numeric scales or percentages option held a clear majority, even compared to the other rank-ordered option. This split may indicate tensions or trade-offs faced by cybersecurity risk managers as they balance precision versus parsimony or weigh the potential organizational costs associated with more quantitative measurements, such as data collection and storage expenses. It likely also reflects spillovers from respondents who claimed to favor quantitative measurements for approach selection but opted for the less granular, rank-order option.

---

[29] Some approaches, such as CIS 18, can effectively complement others, like FAIR, where CIS 18 control categories can map to some of FAIR's risk measurements and functions, creating a mixed qualitative and quantitative cyber risk strategy. Interviewee 15 performed a similar mapping of CIS 18 controls to other enterprise management and project portfolio software for a client company [I15].

Figure 11

Measurement Preference Percentage

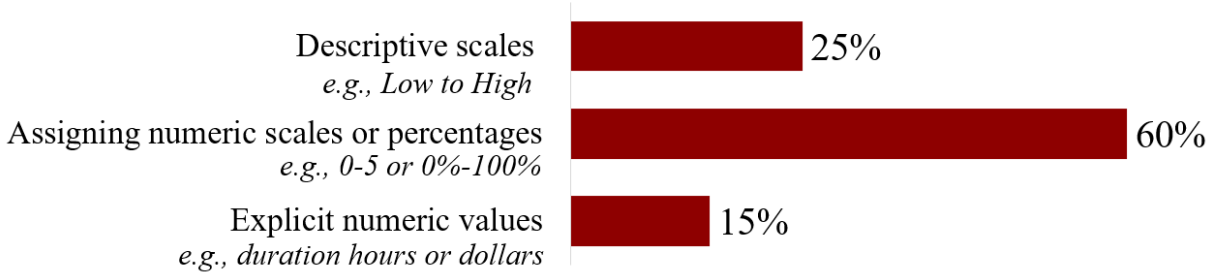


Table 33

Approach Measurement Preferences by Managerial Level

Approach Encounter: Generally Keep Informed

	Middle Mgmt		Upper Mgmt		Executive Mgmt		Total	
	N	%	N	%	N	%	N	%
Descriptive Scales (e.g., Low to High)	27	31	12	26	5	46	44	30
Assigned Numeric Scales (e.g., 0-100%)	53	62	24	51	5	46	82	56
Explicit numeric values (e.g., hours, dollars)	8	9	11	23	1	9	20	14
Total	88	102	47	100	11	101	146	100

Approach Encounter: Learn When Necessary

	Middle Mgmt		Upper Mgmt		Executive Mgmt		Total	
	N	%	N	%	N	%	N	%
Descriptive Scales (e.g., Low to High)	8	23	8	7	1	25	11	16
Assigned Numeric Scales (e.g., 0-100%)	25	71	25	68	1	25	47	67
Explicit numeric values (e.g., hours, dollars)	2	6	2	26	2	50	12	17
Total	35	100	35	101	4	100	70	100

Both Approach Encounters (Combined Total)

	Middle Mgmt		Upper Mgmt		Executive Mgmt		Total	
	N	%	N	%	N	%	N	%
Descriptive Scales (e.g., Low to High)	35	29	14	18	6	40	55	25
Assigned Numeric Scales (e.g., 0-100%)	78	63	45	58	6	40	129	60
Explicit numeric values (e.g., hours, dollars)	10	8	19	24	3	20	32	15
Total	123	100	78	100	15	100	216	100

Table 33 illustrates these differences across levels of management. The table also accounts for a third binary variable regarding how these managers encounter new approaches—they either discover them through their typical routine of staying informed about CSRI&A activities or learn of new approaches as part of an intentional search to meet their organizational needs.

Survey respondents displayed in Table 33 are categorized into three groups based on management type. The smallest of these groups is the executive level. These managers preferred ordinal measures 2:1 over explicitly quantitative measures. This 2:1 trend reverses among executives within the "Learn When Necessary" subgroup. The low frequency of this latter subgroup, consisting of only four participants, necessitates caution in drawing strong inferences from this pattern.[30] Among the full table and the "Learn When Necessary" subgroup, both Executive and Upper-level Managers preferred the quantitative, explicitly numeric values option over their Middle Management counterparts by more than a 20% margin.

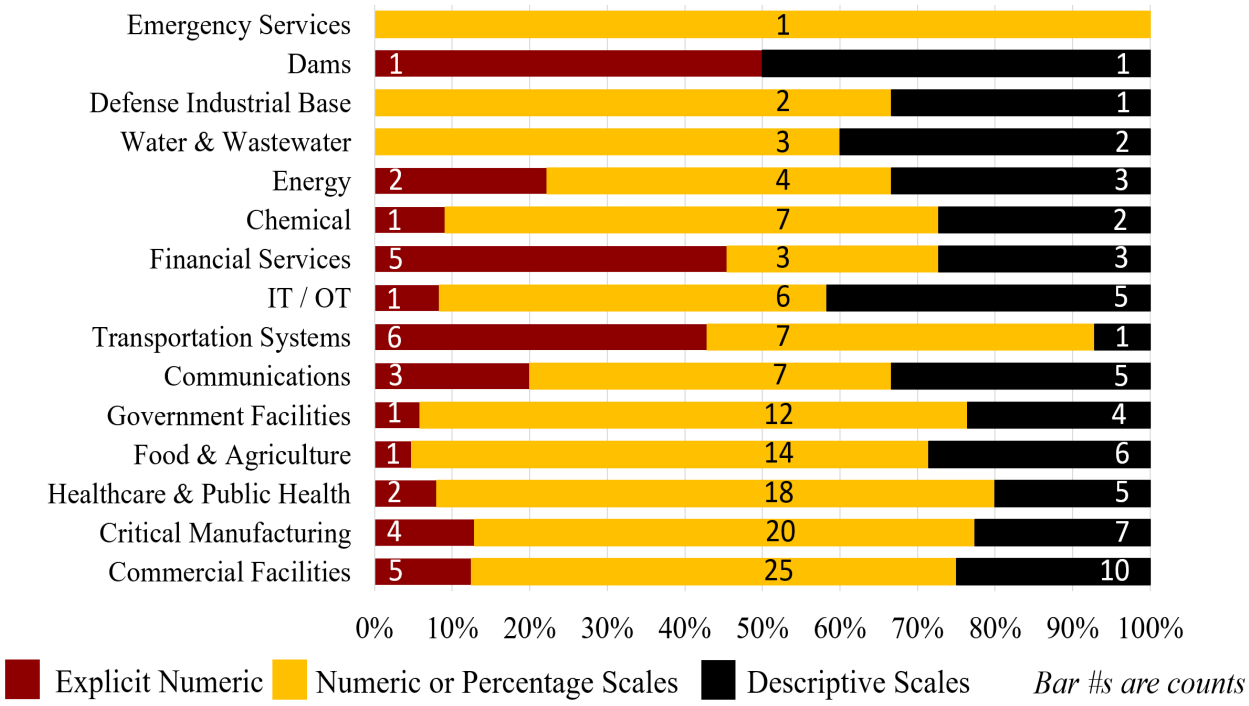
Comparing the 16 critical infrastructure sectors in Figure 12 reveals differences in overall patterns across these sectors. The larger the bar color, the more of an aggregate preference for that measurement group in that sector. To ground the percentage, the numeric value embedded on each color bar represents the number of organizations that chose the approach group and are useful to know when sectors have many or few organizations for comparison. Notably, there are significant spikes in interest for quantitative measurements in the finance and transportation

[30] The managerial level by measurement preference in the approach encounter: Learn when necessary group sub-table showed a statistically significant Chi-Square Test of Independence with $X^2(4, N=70) = 10.75$, $p=0.03$. The full table is also statistically significant, $X^2(4, N=216) = 13.5$, $p=0.01$, but the Generally Keep Informed sub-table was not statistically significant, $X^2(4, N=146) = 6.66$, $p=0.15$. All three Chi-Square results had approximation warnings due to relatively small sample sizes in some table cells.

sectors, at 45% and 43%, respectively. However, the remaining findings do not exhibit any specific patterns.[31] Additionally, managers across most sectors preferred qualitative over quantitative measures by a substantial ratio, typically between 1.5:1 and 2:1. The IT sector showed a ratio of 5:1, while the Food & Agriculture sector had a ratio of 6:1.

Figure 12

Stacked Count Measurement Preference by Organization Sector



5.3.3.2 Tensions and Trade-offs in Measurement

Reflecting on my conversations with cyber professionals, as noted in my positionality statement in Chapter 4, and considering textbook materials such as Hubbard and Seiersen (2016), there is a growing interest in focusing on quantitative measurements—the more specific and

[31] This table is not statistically significant, $X^2(28, N=216) = 33.483$, $p=0.22$.

fine-grained, the better. Conversely, the evidence from this study does not seem to support this perspective. Only about one-quarter of interviewees and survey participants expressed a preference for quantitative measurements, and even fewer cybersecurity managers explicitly endorsed that view when prompted. Instead, assigning numeric scales emerged as the dominant choice, possibly due to efforts to employ methods that could align well with other measurement metrics. This preference may also stem from structural factors or the availability of communication tools for quantitative measurement, which I will detail below.

Regarding this majority rank-ordered response, cybersecurity managers may prefer explicit quantitative measures but find themselves compromising with ordinal measures. It could also be that neither extreme is superior to the other and that they may work best in tandem depending on key aspects of the organization or its processes. This approach allows each to focus on measurement performance and precision. As a director of a large public for-profit financial sector organization pointed out:

> Rather than the qualitative aspect, if you're asking 10 different people qualitatively for an answer, you're going to get different answers based on their experience, and based on how they view things, and their perspective, which isn't bad, but I think it needs to be underpinned by the quantitative data [I7].

This director seems to value multiple, diverse inputs in the process but also recognizes that the less rigid categorical boundaries of nominal and ordinal measures invite more subjective interpretations and response variance. Additionally, this director favors using quantitative data to ground and unify those varied qualitative answers. Together, these insights provide the director with greater context and organizational understanding, informing how they utilize these approaches:

> You can't just take the metrics and go everything's great or everything's bad. You have to actually understand that and put the qualitative lens to it. Underpinning that, the data you can use to underpin decisions will help you more often get to the right decision. I think that that's really a big piece. Then the second piece of it is, because we now have a better compute ability, we're able to monitor, we're able to assess things faster. So, where you might have only visited things every couple of years previously, now you can visit them on a much more frequent basis, sometimes even continuous, or near real-time. [I7]

I contrast this with Hubbard and Seiersen's (2016) position that anything qualitative can be modeled quantitatively (p. 106). While this may be true, there are trade-offs on either side, and ideally, a cybersecurity manager who understands their organization and the end CSRI&A deliverables should be able to determine whether an approach and its measurement methods are suitable for the organization.

Two additional examples demonstrate the tensions in this decision-making process and reflect the gains and challenges of valuing diverse perspectives within the organization. In a more challenging experience, a middle manager from a mid-sized private for-profit communications sector organization shared that:

> Measurements were very difficult for the team to identify then stay on track. We had issues with the [members from] Finance and Insurance not really wanting to participate on defining processes. We had to get all members from the C-suite together to push those two departments. The biggest gap was communication. Standard that was followed was the NIST CSF. [S196]

Interestingly, this manager's organization also employs the ISO-27001 and COBIT approaches, finding the NIST CSF and ISO-27001 sufficient, but not COBIT. Notably, these approaches

offer flexible options for choosing between qualitative and quantitative measurement metrics. It is possible that the Finance and Insurance teams, both typically focused on quantitative measurements, experienced disconnects with other organizational members or disagreed with one another regarding specifics within those metrics. There is insufficient information to determine whether and how flexibility within the chosen approaches may complicate the cybersecurity manager's user experience.

Conversely, a middle manager from a private, for-profit, mid-sized organization in the food and agriculture sector stated that their "decision came from looking at more common threats in our environment and what would set our company up for the most success. Using two approaches helps ensure we're doing everything possible" [S129]. In this case, the two approaches are the SOC-C and CIS 18, both of which the manager confirmed are still in use and deemed sufficient. The SOC-C, rooted in auditing and accounting, incorporates quantitative elements but primarily emphasizes qualitative cybersecurity measurements. Likewise, the Implementation Groups (IGs) within the CIS 18 consist mainly of checklist-type features that contribute to ordinal scales for assessing organizational cyber maturity and risk. This middle manager did not specify whether there were any challenges or pushbacks regarding the selection or implementation of these approaches, although coordinating both the SOC-C and CIS 18 would typically involve multiple teams within an organizational structure.

The middle ground may also be structural. A CIO of a large, quasi-government organization in the energy and water/wastewater sectors discussed quantitative measures as a determinant of cyber maturity, which is formalized in systems like the CMMI and the NIST CSF derived from CMMI. He noted that an organization cannot achieve peak maturity without quantitative measurements [I20]. However, this CIO also explained the potentially steep costs

organizations face, "*unless they've got money out the wazoo to throw, they're still not going to get quite get there"* to implement the systems necessary for full quantitative reporting [I20].

This CIO was knowledgeable about various approaches and multi-sector cybersecurity needs across IT and operational technology (OT) systems. He pointed out that there are diminishing returns with many approaches, such as the NIST CSF tiers and CIS 18 IGs. Consequently, organizations can achieve substantial cybersecurity gains at lower NIST CSF tiers or CIS 18 IGs, but those gains become harder to realize at higher tiers and IGs due to the required types of infrastructure and processes, along with their associated costs. The specifics of the system also matter—for instance, whether it is an Enterprise Resource Planning (ERP) system or a peripheral solution.

Developing and integrating quantitative measures at lower tiers and IGs can be costly, even if done in preparation for higher tier and IG development. Thus, the decision to adopt quantitative measures, and by extension some approaches that rely on those measures, becomes a return on investment (ROI) issue and a topic of discussion in cybersecurity budgeting. At the CIO's organization, the executive leadership:

> Didn't really have an understanding of IT. They looked at risk more from the fiscal side than anything else. They looked at risk as far as project risk, which a lot of organizations do. The cyber risk itself wasn't brought in until [the CIO] started bringing it in with [himself] when they hired their first ever CISO in May of 2020.They brought [the CIO] in here to help build these programs out, help them understand these things. [I20].

Another reason may be perceptions regarding the availability of current quantitative measurement tools. The senior manager of a large, private, for-profit organization in the national defense, government facilities, and IT sectors noted that while quantitative values were

compelling, heatmaps with grouping and color options were more efficient for quick assessments [I22]. Heatmaps are valuable for conveying large amounts of data to leadership who may have less quantitative expertise. This perspective was echoed by a VP of a small, private, non-profit organization in the education, healthcare, and public health sectors, who acknowledged the importance of all three measurement types. Their CEO insisted on using quality incident reporting expressed as a 3x3 matrix [I17]. In this context, the broader row and column matrix groupings provided the necessary perspectives for executive decision-making without the additional effort and cost associated with obtaining pure quantitative precision. Figure 13 illustrates a typical heatmap, where the colors follow a green-to-red gradient, indicating that cyber risk increases as the colors shift toward red.[32] Via this heatmap risk assessment tool, the user evaluates the likelihood (row) and consequence (column) of a specific risk scenario, then locates the corresponding cell in the matrix to determine its risk level classification and suggested response. For example, if an event is judged "Likely (4)" to occur and would have "Major (4)" consequences, the risk is classified as "Catastrophic (16)," signaling the need for urgent mitigation actions.

There are many iterations of the traditional heatmap that enhance its functionality. However, substantial critiques exist against using heatmaps as risk-scoring methods, including Hubbard's (2009) assertion that "all of them, without exception, are borderline or worthless" (p. 122). Evolving visual representations of quantitative measures include increasingly complex data dashboards, such as Tapestry from Decision Point Analytics (2018), featured in Figure 14. Currently, I lack causal evidence demonstrating how the preference for quantitative measurement

[32] From a design perspective, the use of green-to-red colors is a cultural remnant from its origin, where red signifies bad or stop, and green signifies good or go, similar to a traffic light. This color scheme is not visually accessible to all users.

influences the choice of approach, or vice versa. Nevertheless, tools like Tapestry were designed to provide a detailed quantitative framework equipped with graph network features to better support strategic and operational cyber risk management in critical infrastructure organizations. Building off the Tapestry example with the network and data visualization risk assessment tool, the user can analyze how risks propagate through interconnected systems and pinpoint which assets or operations pose the greatest threat of financial loss. For example, by examining the loss exceedance curve on the bottom-right corner, the user can view gradients of steeper risk at lower thresholds, and plan targeted mitigation for select segments and at organizational nodes.

Figure 13

Typical Risk Management Heat Map

		Consequences				
		Insignificant (1) No injuries / minimal financial loss	**Minor (2)** First aid treatment / medium financial loss	**Moderate (3)** Medical treatment / high financial loss	**Major (4)** Hospitable / large financial loss	**Catastrophic (5)** Death / massive financial loss
Likelihood	**Almost Certain (5)** Often occurs / once a week	Moderate (5)	High (10)	High (15)	Catastrophic (20)	Catastrophic (25)
	Likely (4) Could easily happen / once a month	Moderate (4)	Moderate (8)	High (12)	Catastrophic (16)	Catastrophic (20)
	Possible (3) Could happen or known it to happen / once a year	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
	Unlikely (2) Hasn't happened yet but could / once every 10 years	Low (2)	Moderate (4)	Moderate (6)	Moderate (8)	High (10)
	Rare (1) Conceivable but only on extreme circumstances / once in 100 years	Low (1)	Low (2)	Low (3)	Moderate (4)	Moderate (5)

Image: Dasta (2019)

Figure 14

Tapestry, a Web-based Application for Risk Assessment

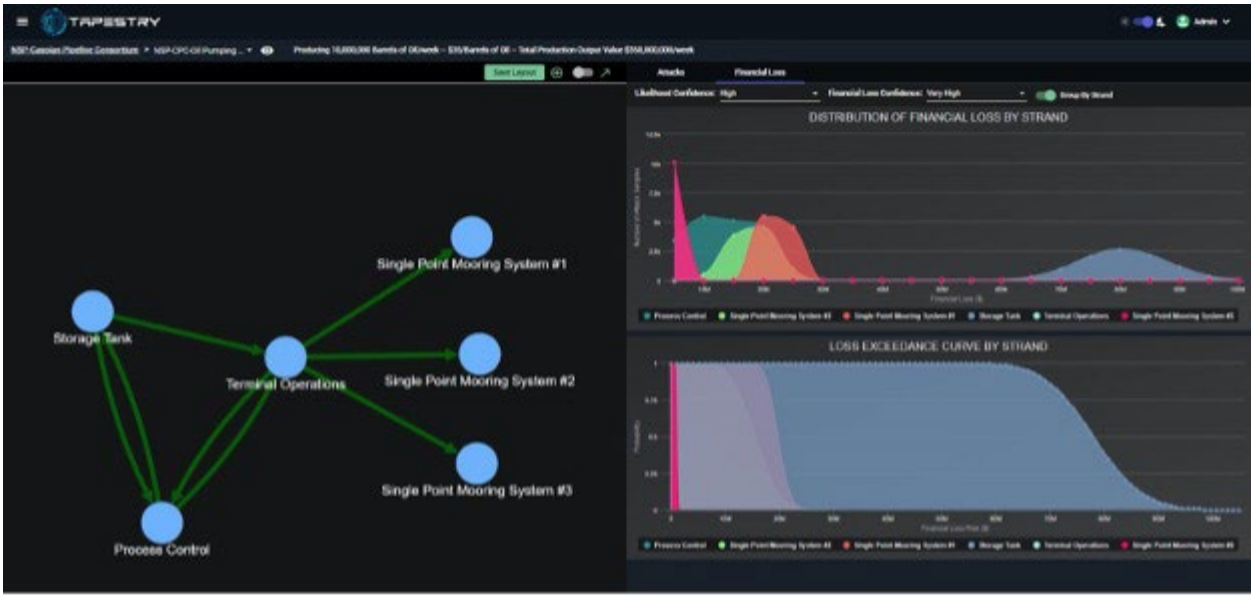


Image: Decision Point Analytics (2018)

5.3.3.3 Risk Visibility and Prioritization

For senior managers, one of the most persistent challenges in CSRI&A is determining which risks matter most and deserve limited resources. As one manager from the DIB noted, "The challenge is prioritization, and limiting the focus of what you're actually trying to address with regard to risk management" [S22]. Qualitative approaches, such as heat maps or ordinal scoring, remain popular because they are broad and easy to communicate, particularly in early-stage conversations. They allow analysts and leadership to quickly highlight "what's okay and what's not," even if the detail is coarse [S17]. However, their weaknesses are well known. One health sector vice president described heat maps as "easy… but wildly inaccurate" [S17], often producing noise rather than clarity.

In contrast, quantitative methods such as the FAIR model are praised for their rigor and their ability to translate cybersecurity threats into business-relevant terms. As one IT sector CTO

explained, “The hardest thing about getting the management chain to agree upon protection mechanisms for whatever risk is identified is putting a financial number to it. So, these quantitative approaches are much better for everybody” [S10]. FAIR serves as a “Rosetta Stone” for many CISOs, providing a “common taxonomy” to articulate risk to boards, finance leaders, and compliance needs [S20].

The practitioner community is increasingly recognizing the value of combining these two approaches. As one energy security executive shared, “If a technical risk assessment is performed and not reported in the same way as other risks, perhaps in dollars, it will fall on deaf ears” [I16]. Blending qualitative clarity with quantitative rigor helps managers maintain accessibility while ensuring decisions are based on defensible evidence. Professional associations like the FAIR Institute, ISACA, and (ISC)² have created working groups and conference tracks that explore this balance, signaling to practitioners that the shift is from “either/or” to “both/and.”

5.3.3.4 Financial and Resource Considerations

Budget justification is a key factor driving the preference for quantitative approaches in CSRI&A. Executives consistently report that financial framing “makes the most sense to a decision maker” because numbers can unlock funding and resource allocation, which is particularly important given the scarcity of public utility sector funds [I22]. One government Chief Information Security Officer (CISO) in the energy sector noted the challenge of securing funds without quantification: “need a way to justify requests for money back to OMB and to Congress, something quantitative that says I’ve had a disciplined approach” [I9]. In commercial settings, quant-focused approaches such as FAIR are often highlighted as well-suited: “It’s all about money, laying out the dollar amounts… and the range of what we think this is going to

cost you. FAIR works really well in a commercial environment," claimed a technology executive with strong ties to the DIB [I5].

However, practitioners also emphasize that quantitative analysis is not always sufficient or even feasible. Some risks cannot be fully captured in financial terms, particularly in mission-driven or public sector organizations. One healthcare executive described this gap: "Financially not that bad… but someone died on the other end. That's against our mission" [I17]. In such contexts, approaches that provide qualitative narratives, scenario analyses, and hybridized measurement options are essential for framing resilience, mission continuity, or life-safety concerns that resist monetization. Professional communities, such as ISACA's Risk IT group, emphasize that qualitative framings help avoid over-financialization, ensuring that security leaders do not lose sight of values beyond budget lines (Redlein et al., 2023). Meanwhile, PricewaterhouseCoopers (PwC) highlighted the importance of qualitative elements within the International Auditing and Assurance Standards Board (IAASB) standards for the ISSA 5000 approach used for audit disclosures to better capture materiality (PwC, 2025).

Nonetheless, the tension between the need for quantitative evidence and the reality of qualitative framing reflects an ongoing maturation in the field. As a healthcare VP summarized, "Over time, it's gone from pure qualitative and heat maps to qualitative and quantitative" [I17]. This hybrid trend mirrors the evolution of cybersecurity itself: moving from compliance-driven reporting toward integrated risk management aligned with enterprise financial planning. Ultimately, understanding the perceived and actual measurement preferences of cybersecurity managers is crucial, as it influences how approaches are viewed, adopted, and implemented. Approaches considered too complex or resource-intensive may not be selected, potentially by the cybersecurity manager or by those influencing the budget. Moreover, companies that develop

tools to measure client systems and assets will benefit from understanding the preferences of their potential customers. This knowledge can help developers tailor new products appropriately, and it can inform the data and technology literacy campaigns needed to shift managerial sentiment regarding available measurements and tools. Currently, ranked measures, such as numeric scales, appear to be the preferred measurement method; however, we cannot overlook the fact that cybersecurity managers utilize multiple approaches to meet their needs.

5.3.3.5 Reputation and Trust

While finances dominate board discussions, reputation and trust remain equally critical areas where qualitative and quantitative approaches intersect. Stakeholder trust can be fragile; a government energy CTO noted, "When you don't say 'here's how we'll mitigate risk'… you lose trust, faith, credibility" [I1]. In such cases, qualitative communication tools, such as one-page summaries, simple scoring, and narrative framing can be powerful for maintaining stakeholder confidence. Indeed, a C-suite cyber advisor cautioned that most executives "have the attention span of a gnat" [I14] and require only three clear options or colors to make sense of risk reporting. Communication, attention, and perception can significantly shape trust; therefore, selected approaches must be able to meet this range of needs. An executive with deep familiarity with ISACA shared:

> Perception is reality in our modern-day cybersecurity [and] this is important to me… for how I define risk is both the objective and subjective impact, detrimental impact on an organization [I11].

Yet reputation and trust are not merely subjective. Quantitative methods are increasingly employed to assess brand value-at-risk or to model the financial implications of reputational damage. One executive described using Monte Carlo simulations to analyze confidentiality and

reputation issues, producing loss exceedance curves [S17]. Similarly, models such as FAIR, NIST CSF, and MITRE ATT&CK have been deemed "useful to business leaders," particularly regarding "types of risk assessments [with] more effective communication tools for higher-level executives and boards" [S11], and "telling the board that if you go to court and something happens, you need to have a defensible position" [S16].

This dual use, narrative stewardship on one side, financial modeling on the other, illustrates why reputation management sits at the center of CSRI&A practice. Organizations such as (ISC)² and the SANS Institute have published practitioner-facing case studies on reputational risk in areas like ICS security (Lee et al., 2024) and product supply chains (Turner, 2025). Additionally, industry associations like the National Association of Corporate Directors (NACD) emphasize that boards now expect cyber risk discussions to address both financial exposure and stakeholder perception (NACD, 2023). In practice, CSR managers find that choosing approaches based on qualitative and quantitative elements comes down to balance, resources, credibility, and prioritization, often opting for multiple methods to address a range of needs.

5.3.3.6 The Qualitative-Quantitative Practitioner Community Contribution

Taken together, these findings underscore that CSR managers are neither abandoning qualitative methods nor fully embracing quantitative models. Instead, they are actively blending the two—utilizing qualitative approaches for speed, communication, and mission framing, while applying quantitative methods for financial justification, prioritization, and resource acquisition. This hybrid perspective reflects the growing maturity within the profession, which has been voiced repeatedly across practitioner communities. The professional organizations that support CISOs, cyber risk officers, and IT/OT leaders, such as ISACA or ISSA, along with specialized communities like the ISACs, and sector and executive leadership groups like CISO lunches, all

serve as hubs where practitioners exchange lessons on navigating this balance across different industries.

The qualitative-quantitative contribution to the field is not merely the discovery of new approaches or the dominance of certain methods. Instead, it lies in validating the experience of cyber practitioners: CSR managers require both approaches, tailored to their specific context, to make CSRI&A effective. By recognizing this hybrid model and codifying it within professional forums, we advance the collective knowledge of the community and enhance organizations' ability to manage cyber risk with both rigor and clarity.

5.3.4 Compatible or Conflicting Approaches: NIST versus ISO

The choice of quantitative measurement strategies—whether ordinal, interval-ratio, or tools like heatmaps—shapes how risks are identified and prioritized, influencing the credibility and impact of risk management decisions within organizations. These technical differences are far from trivial; they reflect deeper debates about comparability, consistency, and the underlying objectives of cyber risk analysis. As measurement approaches become more sophisticated, the options and complexity increase, prompting managers to consider which methods or combinations best meet their RI&A needs, regulatory expectations, and operational realities. This next section explores the compatibility and conflict between leading cybersecurity standards, focusing on how organizational context, stakeholder pressure, resource constraints, and management levels foster both convergence and divergence, primarily between NIST and ISO.

An interesting finding is the comparison between the NIST and ISO approaches. Both are globally recognized standards among industry and government, and together, they are among the most popular cybersecurity risk-based frameworks (Kurii & Opirskyy, 2022; Ramirez et al.,

2020). Additionally, both NIST and ISO are unique in this study as they comprise a suite, or family, of related standards. As standards, they signal to various users and stakeholders that adherence to them ensures a certain level of security, performance, and reassurance based on what those standards dictate. Unlike a framework or model, which can be implemented in various ways, a standard should be applied consistently.

From my survey, I found that interview data reflected a strong preference for NIST-based approaches, with nearly 60% of interviewees currently using at least one NIST product and another 13% having had NIST products suggested to them. However, results in Table 34 indicate that cybersecurity managers selected ISO approaches by a 12% margin over NIST approaches. Yet, the marginal advantages ISO has over NIST concerning approach selection may not remain a compelling argument for sustained use. Figure 12 illustrates the current application of these combined ISO and NIST approaches. While ISO offers slightly more total approaches than NIST and a similar number of approaches that are still in use and deemed sufficient, it has nine more approaches (18%) that are no longer in use and 11 more approaches (31%) that are still in use but considered insufficient. Therefore, although ISO initially attracted more interest in approach selection, it also experiences a higher rate of abandonment compared to NIST. ISO shows a greater number of insufficient yet sustained uses relative to NIST.

5.3.4.1 Location and Regulation

Factors influencing the initial selection and retention of these approaches may include compliance requirements, perceptions of performance, adoption and substitution costs, and opinions about the approaches and their parent organizations. Selection between NIST and ISO is partially driven by regulatory requirements, such as those faced by Participant I11's contacts in Europe, and Participant S136 in critical manufacturing, who adopted ISO approaches for

compliance reasons. Similarly, many NIST approaches, including the RMF, are mandated for use within the US federal government as it is the federal agency for standards development. Compliance can also intersect with other infrastructure sector requirements. For instance, Participants S2 and S3 in the healthcare sector were required to adopt NIST approaches alongside HIPAA regulations. Organizations in these sectors may find ISO or NIST approaches sufficiently useful but are unlikely to abandon them without regulatory changes.

A director within an accounting firm's security team, who also serves as a senior consultant for the firm's clients, reflected:

> Earlier on, we were building our stuff more explicitly out of ISO 27001. We found it doesn't go down the rabbit holes in a way conducive to managing the rabbit holes. The NIST Cybersecurity Framework does, frankly, a much better job [I15].

This trend is reinforced by compliance mandates: ISO is popular in Europe, while NIST remains the default in US federal, healthcare, and finance sectors. A surveyed executive from a financial services private non-profit organization stated, "Mostly align to NIST CSF as it has become the de facto standard in the US financial sector. IT uses COBIT. Cybersecurity used many NIST standards." [S14]

For organizations not bound by relationships with respect to ISO or NIST, these frameworks may be adopted based on their merits. According to Interviewee 15, a cyber educator and former information security director of an accounting firm, "the NIST cybersecurity framework does, frankly, a much better job. Given that I think almost all of our clients are US-based and almost all of their work is US-structured, following NIST is more appropriate for that" [I15]. Although "better" is subjective, Interviewee 11, a technology company director, noted, "NIST is a little more granular, but you can get over-granular" [I11].

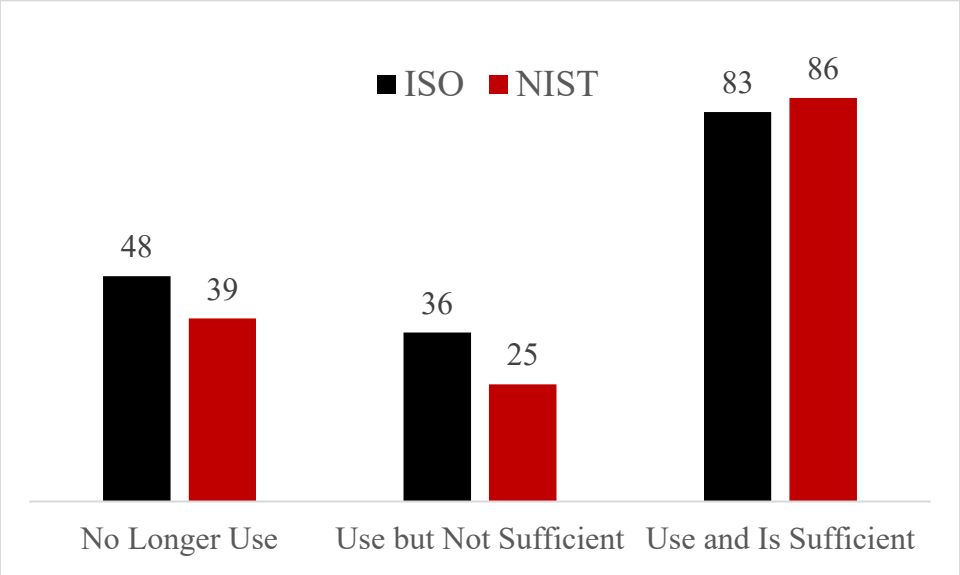
Table 34

Comparing ISO and NIST Approaches Selected by Survey Participants

ISO					NIST				
Rank	Approach	N	Sum (N) %	N /216 %	Rank	Approach	N	Sum (N) %	N /216 %
1	ISO 27001 &/or 27002	113	68	52.3	3	NIST SP 800-53	51	34	24
6	ISO 27005	42	25	19.4	5	NIST Cybersecurity Framework (CSF)	43	29	20
15	ISO 31000	10	6	4.6	8	NIST SP 800-37 Risk Management Framework (RMF)	21	14	10
24	ISO 21434[+]	2	1	0.9	11	NIST SP 800-171	13	9	6
					16	NIST SP 800-82	9	6	4
					18	NIST SP 800-39	7	5	3
					21	NIST SP 800-30	5	3	2
	Total	167	100	77.3		Total	149	100	69

Figure 15

Survey Participant Counts of ISO and NIST Approach Current Use Status



5.3.4.2 Costs / Finances

Measuring "good" in terms of direct financial costs, both ISO and NIST offer extensive publications on their approaches at varying prices. As Participant I11 repeatedly stated, "NIST is free," whereas with "ISO controls, I have to pay just to come online" [I11]. Relating back to the requirements for adopting these approaches, cybersecurity services CISO Participant I21 echoed concerns about cost-based barriers to entry and participation within infrastructure sectors, describing pay-to-play requirements as "suffocating" and stating they "don't help organizations be more secure … or risk averse" [I21].

Adopting an approach can incur additional administrative, financial, and human capital costs. I11 pointed out that they used both NIST and ISO products based on client requests: "The client wanted NIST stuff. They wanted ISO stuff. So, we did an alignment for NIST and ISO and so forth. And that is what we then codified, because that's what they asked for" [I11]. Meeting client and internal needs to incorporate these approaches requires personnel who understand how to utilize them. Claiming "not the expert" status for the NIST CSF, Participant I7, a cybersecurity services director, stated, "I hired people whose whole professional purpose in life is to implement the NIST cybersecurity framework and to assess it, so we have a team dedicated to that assessment capability." While not using ISO approaches in their entirety, Participant I7 also acknowledged "leveraging portions" of ISO 27000 along with the NIST RMF to "coalesce all those things," and noted "knowing other institutions that do the same."

Accessibility and cost significantly influence framework choices. NIST's public availability is frequently cited as a key advantage for both smaller and larger organizations, while "ISO often requires paid access, and that's exclusionary for small orgs or startups trying to do the right thing," claimed a long-time DIB security executive with consulting expertise [I21].

These financial and logistical barriers are not merely incidental; they often determine whether an approach is widely adopted or quietly sidelined. “We’re constantly mapping our reference standards back to NIST, CIS, and HIPAA… but ISO gets dropped when the client has no need or can’t justify the added cost. And most of our clients are US-based, so NIST is simply a better fit,” noted another expert [I15].

Bespoke and adaptive frameworks have emerged as a pragmatic middle ground, allowing organizations to adopt elements of both NIST and ISO. This integration of client mandates and sector-driven requirements results in flexible, bespoke frameworks that can satisfy multiple audits with minimal redundancy [I17]. This “adopt and adapt” mentality fosters resilience: “We build reference standards so that when you take them all together, you can find NIST CSF in it, you can find HIPAA in it… it’s sort of a ‘Franken-framework’” [I17]. However, this flexibility incurs costs in terms of diverging terminology and the labor required for cross-mapping, which can lead to confusion or compliance fatigue if not carefully managed.

Public cybersecurity professionals, such as cybersecurity bloggers, help alleviate confusion and fatigue regarding approach selection through educational posts designed to inform and guide. For example, CISO and risk manager Luigi Sbriz compared the internal control aspects of ISO/IEC 27001:2022, NIST CSF 2.0, and Risk Treatment Plan on the ISACA blog (2024). In his review, he proposed CMMI as the best approach for control activity evaluation and gap analysis due to its broad applicability and simplicity (ibid). In contrast to Sbriz’s short-form post, the Retail & Hospitality ISAC (RH-ISAC) stated that the NIST CSF “remains the gold standard” based on adoption estimates, rather than making a targeted case (Chambliss, 2025). Notably, both sites reach different segments of the CSR manager community. Sbriz’s post on ISACA targets an individual-based, sector-agnostic membership of cyber professionals and

cybersecurity credential seekers, while RH-ISAC focuses on institutional memberships from organizations within the Retail and Hospitality sector, although interested individuals can still follow along. Although I lack readership metrics for these posts, it is reasonable to suggest that the size, scale, targeted audience, and messaging of the person or organization sharing can influence approach selection—something that warrants future analysis.

5.3.4.3 Brand Loyalty

The preference for NIST over ISO may involve brand loyalty based on users' positive experiences with the approach developer. Participant I7 stated that their relationship with NIST "was built because NIST asked for input on everything. I did a lot of work with NIST over the years, and the fact that they take input from everybody." [I7] They continued:

> If you've ever looked at the comments, the comments are all public on every draft publication… you read the occasional comment that's idiotic, and NIST still reads it and responds to it, and [name redact] really liked that. In so many of the others, it's like if you're not on this committee, nobody cares. You have no input. This is what's going to happen, and these are the standards coming out. So that's why [name redact] liked this so much, because NIST solicits input from industry, and NIST takes it seriously. They adjust accordingly based upon what they feel is the most insightful and the best reasoning from industry on something. [I7]

Yet, that same participatory design can have both negative and positive effects. When discussing the long waits for approach updates, I14 remarked, "NIST is very slow, but they're very good." [I14]

Ultimately, allegiance to NIST is often supported by the participatory and transparent processes that shape its evolution. Many managers described being invited to submit public

comments or participate in working groups, which, according to a CXO advisor and executive from the DIB and IT sectors, "builds trust in the final product—though the slow update cycles do frustrate us at times" [I14]. While ISO is valued for its rigor and international legitimacy, interviewees perceived it as less participatory. Some view its adoption as a necessary concession for global or sectoral reach rather than a strategic first choice. As Participant I15 stated, "We look at ISO, we try to stay current, but we follow NIST—unless our clients specifically demand ISO, which is rare" [I15].

Conversely, survey participants expressed strong support for ISO. These participants were mid-level managers at large organizations, seemingly in more specialized roles. One highlighted the importance of "CPS within the automotive industry [with] cybersecurity standard ISO/SAE 21434" [S10], while another, who managed commercial facilities in the real estate sector, utilized ISO 27001/2 based on "regulatory processes in place" [S105]. A third mid-level manager from the food and agriculture sector employed ISO 27005 in collaboration with their audit team. These differences suggest additional nuances between executive and lower levels of CSR management.

5.3.4.4 Equivalent / Code Switching

Some organizations find the main features of the NIST and ISO approaches equivalent enough that comparison is less of a concern. A maritime transportation services senior advisor stated, "We're agnostic. […] We use NIST, and honestly, it doesn't really matter. There are other risk frameworks within the maritime environment. […] The bottom line is, pick a standard, follow the standard" [I18]. They continued to note that many NIST and ISO approaches share common roots. "People don't realize ISO was baked into a lot of the NIST documents from the beginning," said Participant I20, a CISO at a public water utility. This suggests that

organizations may find it easier to switch between the approaches or even use them simultaneously to meet various customer requirements. Low-cost transitions between NIST and ISO could represent a form of sociotechnical code-switching among cybersecurity managers. Technical code-switching at the organizational level may extend previous individual-level research, such as Downey and Lucena's (2006) work on engineers' professional identity as they navigate transnational spaces. Additionally, forms of technical code-switching may be more common between standards regimes that have established joint standards bridging professional communities, as often occurs between ISO and International Electrotechnical Commission (IEC) or ISO and Society of Automotive Engineers (SAE). As noted earlier, two respondents from the automotive sector separately entered ISO 21434, which pertains to road vehicle cybersecurity, but it would have been equally appropriate for them to enter SAE 21434 or ISO/SAE 21434, as this is a jointly published international standard (Weisenberger, 2021).

In summary, comparative experience with NIST and ISO standards illustrates how regulatory requirements, financial accessibility, and perceptions of developer responsiveness converge, while subtle differences by management level diverge to shape both initial adoption and long-term use. Many organizations, especially those serving diverse sectors or international clients, maintain bespoke programs that synthesize strengths from both frameworks while responding to compliance environments that rarely align neatly. Variation in operational duties, further influenced by who else engages in the RI&A use process, holds significant sway.

Discussions on compatibility and conflict revealed how different cybersecurity approaches can align in practice and where they may create friction for organizations. These analyses highlighted not only the technical overlaps between frameworks but also the inherent limitations of one-to-one comparisons. While compatibility provided insights into how

approaches could be layered together, and conflict identified areas where tensions undermine effectiveness, these perspectives remained limited to surface-level contrasts. The next step is to move beyond these pairwise evaluations and examine how organizational realities and managerial traits collectively shape the decisions made in practice.

5.3.5 Association Rules for Approach Selection based on Managerial and Organizational Traits

So far, there have been meaningful differences in approach selection through the use of consultants, distinctions by measurement preferences, and approach compatibility. Richer, more nuanced associations emerge when viewing groups of managerial and organizational traits acting together. This section is the most experimental part of my study, where I seek multivariate interaction results obtained through association rules data mining techniques applied to the managerial and organizational traits on approach selection. As introduced in Chapter 4, association rules produce if-then patterns between variables called rules based on how often traits appear together in the data at the same time.

A primary output of this work is the development of managerial trait profiles that can be used to further study approach selection and design. Further quantitative work can store profile data as vector column data for computational models, and qualitative researchers can leverage profiles to create User Experience style personas. In both cases, the key to understanding these profiles is the managerial and organizational traits that comprise them and help determine the chance of selecting specific approaches based on those traits.

Recall from Chapter 4 that association rules are statements that describe how the presence of certain items or traits (the “if” or left side, known as the antecedent) is linked to the occurrence of other items or traits (the “then” or right side, known as the consequent) within a transaction dataset. The rule itself is a directional statement that specifies which items or traits

are on the antecedent and which are on the consequent side. Itemsets, on the other hand, are simply groups of items that frequently appear together in the data, without any implication or direction. Association rules are constructed from these frequent itemsets by dividing them into antecedent and consequent parts, allowing us to analyze and summarize co-occurrence patterns and directional relationships among elements in the dataset.

5.3.5.1 Association Rules Setup

In my study, the rules and itemsets derive from managerial and organizational traits, with trait data coming from the survey participants. Example surveyed traits include managerial demographics like hierarchical level in their organization or frequency of CSR duties, or organizational traits such as organizational profit type or which groups in the organization perform CSR duties. The traits also include responses to a 60-item series of modified TAM 3 Likert statements regarding the importance of why the managers use their selected approach for their organization's CSRI&A activities.

Each variable in the association rules analysis is a binary indicator, signaling if that trait is present when it appears in an itemset and rule. From the survey data, I derived 110 binary trait variables recoded from the three types of survey data. The first are already binary, such as whether the manager's organization is a member of the Auto-ISAC or not. Similarly, the second binary type is analogous to regression dummy variables, such as splitting organization size variable with five size levels and making five binary trait variables, one for each organization size. The third type derives from numeric variables, where I used a cut point to define the binary state; for example, one binary trait is true if the manager uses more than the average number of approaches.

Reworking my association rules primer example from Section 4.2.4.1, I have shifted the focus from itemsets about bread and jelly co-occurring with peanut butter to itemsets based on my survey data of cybersecurity managers. In my analysis, the left-hand side (antecedent) of each rule represents one or more manager traits—such as keeping informed about new approaches, preferring qualitatively descriptive scales, or having an above-average score on a TAM-style price-value construct. The right-hand side (consequent) of each rule always consists of a single organizational approach, such as NIST SP 800-171. By structuring the rules this way, I can directly assess which combinations of manager traits most frequently co-occur with the use of individual cybersecurity approaches within organizations.

As the number of left-side variables increases, the number of potential itemsets increases exponentially. I set the left-side limit to five variables to help ensure that the resulting rules remain understandable and actionable for decision-makers, as rules with too many variables can become overly complex and difficult to interpret. The association rules ran the Apriori algorithm with the same restricted settings for all managerial and organizational traits and approaches.[33] I kept the top 100 rules sorted high to low on the lift metric for each approach.[34]

---

[33] To recap, support is the proportion for when left and right-side items appear in the data. Confidence is the proportion of how often the right-side item appears when the left side item(s) occur. Lift is a likelihood ratio for the right-side item appearing with the left side item(s) beyond random chance alone (confidence / support). I lowered the minimum metric thresholds to help obtain meaningful rule pairings. The restricted (default) values were support = 0.01 (0.1) and confidence = 0.1 (0.8). I also set the minimum number of items in a rule to 1 (1) and maximum to 5 (10). 5 is typical cutoff value to keep results manageable; for comparison, Oracle's association rule guide has a default cutoff at 4 variables (Wang et al., n.d.).

[34] Math clarification: Given the rule constraints above and up to 110 binary traits, for each approach, there are a possible 633,245,831 rules, where $Total\ Rules = \sum_{k=1}^{5} \left(\frac{110}{k}\right)$. Not all approaches reached the maximum amount, as most rules could be discarded due to low association metrics and viable results could still yield thousands of rules. I only kept the top 100, sorted by the lift ratio, since lift is ideal for discussing trait occurrence by random chance. 100 rules is a general best practice value for preliminary sifting when using large data results.

In the following subsection, I introduce a case example of the FAIR approach using only a few rules as an initial demonstration for interpreting the trait pattern results and how I use them to construct a user profile. Afterward, I provide an overview of traits and lift ratios for each approach profile, followed by discussion of four approach profiles before moving onto viewing select traits across approaches.

5.3.5.2 FAIR Approach Profile Example - Eight Rule Example Profile

As a new method applied in CSRI&A approach selection, this subsection serves as an initial example using FAIR to compare common traits across rules to make a smaller, starter profile before I move on to aggregating them by all 100 rules by that approach. The number of traits within a rule varied from one to five, with most having two or three traits. For example, Table 35 contains the following top eight rules from the FAIR approach. I display eight-rules here because they all share the same rule metrics, with some variability in the traits across those rules, making them easier to compare and discuss equally (support = 0.014, confidence = 1.0, and lift = 30.86).

The analysis of association rules demonstrates the value of developing selection profiles based on recurring managerial and organizational traits. For example, recalling the previous chapter, the FAIR approach consistently aligned with executives possessing 21+ years of experience, often in for-profit settings, and with managers who actively stay informed about emerging methods. For consultants, such profiles offer a blueprint for tailoring recommendations, enabling them to anticipate which approaches might resonate best with leadership demographics and styles or organizational types and cultures. Instead of treating approaches as static products, consultants can design bespoke or hybrid approaches that align more directly with a client's leadership structure, organizational elements, and resources. Thus,

the logical assumption is that this not only increases approach adoption and use success but also builds credibility with the CSR manager and other stakeholders who see their unique realities reflected in the recommendations.

Table 35

FAIR Approach Top Eight Rules Sorted by Lift

	Rules (1=First)									
Trait	1	2	3	4	5	6	7	8	N	%
Cybersecurity insurance req. influence choice more than the average		X				X			2	25
Internal Acct & Finance Involved							X		1	13
Mgr Degree: Comp Sci/IT	X		X	X	X			X	5	63
Mgr Exp.: 21+ years	X	X		X	X	X	X		6	75
Mgr Level: Executive	X	X	X	X	X	X	X	X	8	100
Org: For-Profit					X	X	X	X	4	50
Org outsources its CS RI&A			X	X				X	3	38
Number of traits in rule	3	3	3	4	4	4	4	4		

Building on this initial FAIR reduced profile example foundation, the remainder of this section has two parts. The first part reviews overall trait and lift ratio metrics for broader assessment of all the approaches in the study. The second part discusses five additional profiles derived from association rules – FAIR with the rest of its traits considered, NIST SP 800-30, NIST-800-37, ISO 27005, and Custom Approach. I selected these five because their profiles loaded with traits well for comparison, are among the most well-established and widely used approaches, and custom held the largest, unexpected findings. They have a unique combination and differ to the total number of variables, as well as having good potential for emergent profile themes that offer new perspectives on approach selection. By examining these profiles in detail, the analysis aims to further clarify how distinct managerial and organizational patterns shape the adoption and sustained use of cybersecurity risk management frameworks.

5.3.5.3 Combined Approach Association Rules Overview

Table 36 contains a summary overview of traits on analyzed approaches. Approaches with low counts in the # Traits column, such as NISTIR 8286, OCTAVE, NIST SP 800-30, or FAIR, reflect tighter cohesion and association of traits related to that approach. Conversely, approaches with many traits, such as CIS18/CSC, ISO 27001/1, NIST CF, and MITRE ATT&CK reflect a diverse range of possible combinations. The number of managers who selected those approaches can affect this frequency, as more managers present more opportunities to have more and diverse traits.

The minimum and maximum lift values in Table 36 denote the weakest and strongest connections found between the approach and the traits. Recall lift pertains to the likelihood a manager would choose that approach given that rule's combination of traits compared to if they did not have those traits. Some approaches, such as CMMI OR COBIT have the same minimum and maximum lift, which shows there is little to no variation in how strongly different itemsets of traits are associated with that approach. This tends to occur when the findings are consistent for that approach or when there are only a few rules, with the latter not being an issue here. On the other hand, approaches like FAIR or CMMC with different minimum and maximum lift values means that the strength of connection across different trait itemsets varies. Some combinations are much more strongly linked to those approaches than others, suggesting broader diversity in how that approach is associated with different traits. This could indicate that approaches with wider lift ranges are selected for a wider variety of situations or by a more diverse group, while the other approaches are linked to more specific or consistent patterns.

Table 36

Traits and Lift by Approach

Approach	# Traits*	Min Lift	Max Lift
CIS18 / CSC	61	2.77	2.77
CMMC	35	9.60	12.00
CMMI	16	16.62	16.62
COBIT	41	5.02	5.02
Custom	17	9.82	36.00
FAIR	12	5.61	30.86
ISO 27001/2	60	1.91	1.91
ISO 27005	37	5.14	5.14
ISO 31000	23	5.08	12.96
MITRE ATT&CK	46	7.20	7.20
MITRE Shield / Engage	18	9.82	27.00
NIST CSF	48	5.02	5.02
NIST SP 800-171	29	7.12	16.62
NIST SP 800-30	11	4.32	21.60
NIST SP 800-37 RMF	21	10.29	10.29
NIST SP 800-39	19	10.29	23.14
NIST SP 800-53	41	4.24	4.24
NIST SP 800-82	24	2.77	18.00
NISTIR 8286	5	5.40	6.48
OCTAVE	8	5.59	8.10
PHA	23	16.62	16.62
SCF	22	8.31	16.62
SOC-C	27	4.53	11.78

*Note: * Each approach had 100 rules except NIST SP 800-30 (58), NISTIR 8286 (5), and OCTAVE (24).*

5.3.5.3 FAIR Approach Profile

Figure 16

FAIR Approach Profile - Most Frequent Traits from Top 100 Association Rules by Lift

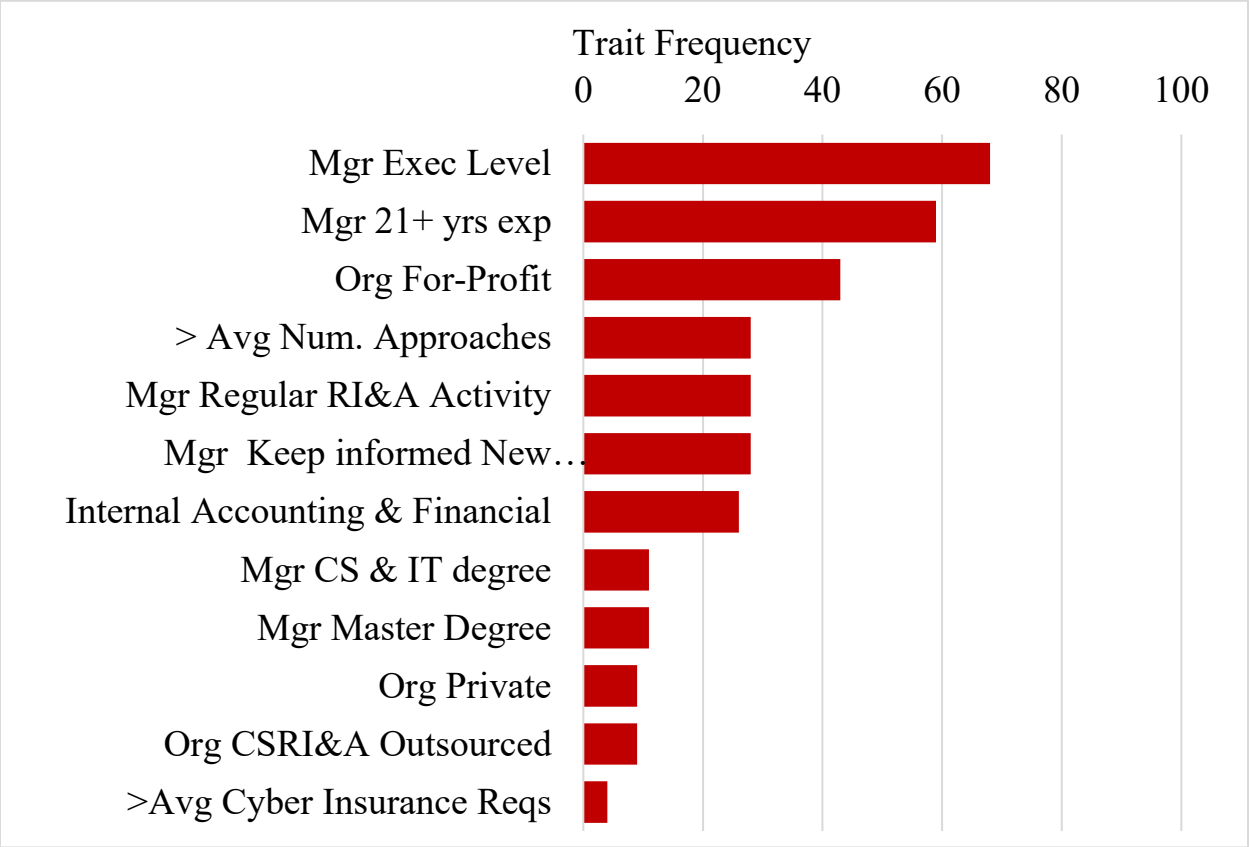
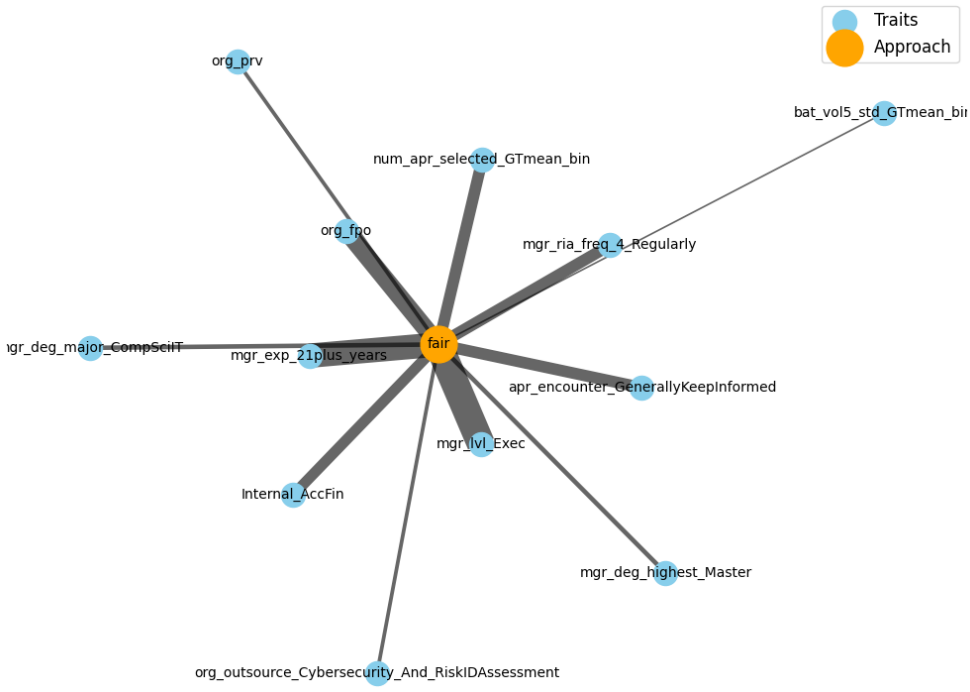


Figure 17

FAIR Approach and Top Traits by Frequency as Bipartite Ego Graph Network



Note: Edge lines thicken as trait frequency increases.

When considering only these first eight rules as an example, the results show several patterns for choosing the FAIR approach. First, choosing FAIR is associated with several traits, as more rules have at least three traits. Second, a selection profile emerges based on which of the 110 traits appear in the top rules and the frequency of those traits. Executive managerial level is the most consistent trait of FAIR, as it appears in every rule. Having 21+ years of experience and a Computer Science/IT degree are also very strongly associated. The years of experience and reaching an executive level are also likely associated, but not immediately relevant here. Working in a for-profit organization has a moderate association, while organizations outsourcing their CSRI&A is somewhat associated. The Internal Accounting & Finance Involvement and Cybersecurity Insurance Requirement Influence are of interest but not strong predictors.

All eight rules had the same exceptionally high 30.86 lift ratio, interpreted as indicating that when a manager has one of these rule combinations of traits, the chance of selecting the FAIR approach is 30.86 times higher than if they did not have that rule's set of traits. This has practical implications for decision making. The more often these traits appear and co-occur across rules for the FAIR approach, the more consistent and reliable they are as predictors beyond random chance expectations, but they do not imply causal relationships.

Results from the FAIR approach show that trait-based profiles can be derived from viewing a series of trait itemsets from association rules. However, forming these profiles should consider more than just the top-most rules, as the constructed profiles may change with more rules. When accounting for all top 100 rules by lift, as shown in Figure 16, the FAIR approach has 12 traits to construct the profile, up from the seven traits across eight rules in Table 35. The executive level and 21+ years of experience remain strongly associated with the FAIR approach. The for-profit organization type is also highly associated, with a slight drop down to 43 rules, from half the rules in the more limited top eight rules. The next strongest predictor traits, which are somewhat associated with this profile, include using a greater than average number of approaches, managers that regularly perform RI&A duties, managers who discover new approaches by generally keeping informed, and teams that work with internal accounting and financial companies. These are newcomer traits to the FAIR approach manager selection profile, other than the internal accounting and financial companies. On the flipside, having a Computer Science/IT degree, which was a very strong predictor in the limited top eight rules, becomes far less influential among all 100 rules and appears only 11 times.

Taken together and rewritten as a managerial selection profile, the typical CSRI&A manager who selects the FAIR approach is often an executive-level leader and/or has over 21

years of experience in their field. This manager is also commonly found in for-profit organizations and is likely to be broadly and regularly informed about new approaches, which may also lead to them using multiple RI&A approaches at once. They are also likely to regularly engage in RI&A activities and include their internal accounting and finance teams. Although advanced degrees and computer science/IT majors are associated, they are less dominant traits. Overall, this profile reflects a seasoned, proactive executive in a dynamic, for-profit environment, who values innovation, comprehensive risk oversight, and collaborative governance.

Figure 17 is an ego-centric network graph of the FAIR approach and top traits from the association rules. As an ego network, all associated traits connect to FAIR at the center, and the edge thickness increases with traits frequency. Results here generally mirror the FAIR approach bar plot above through a different visualization tool with a small amount of new information through this format. I included it to show its overall shape. Trait charts for the other approaches will have overlaid network graphs as well.

5.3.5.4 NIST SP 800-30 Association Rule Profile

Figure 18

NIST SP 800-30 Approach Profile - Most Freq Traits from Top 100 Association Rules by Lift

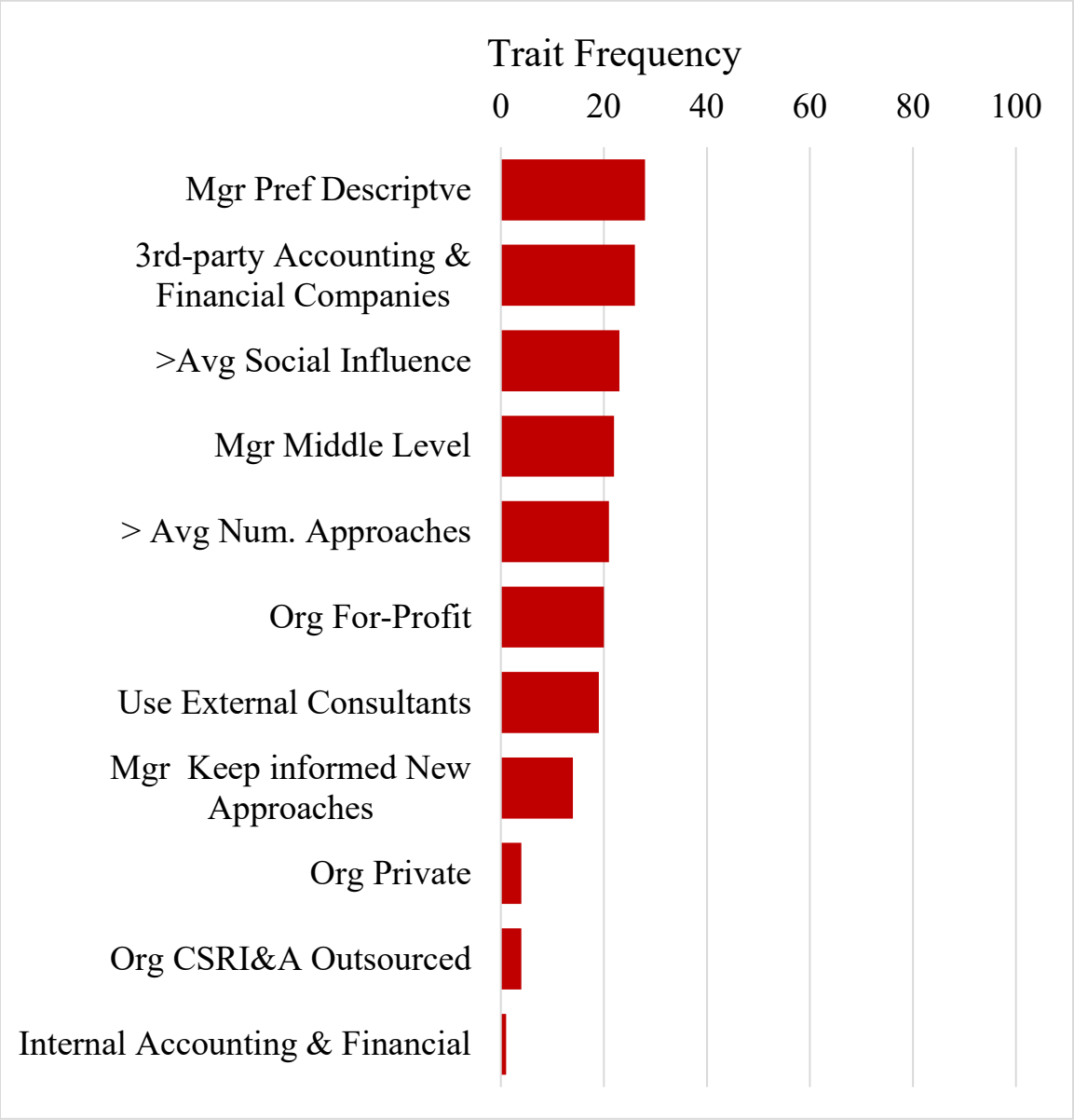
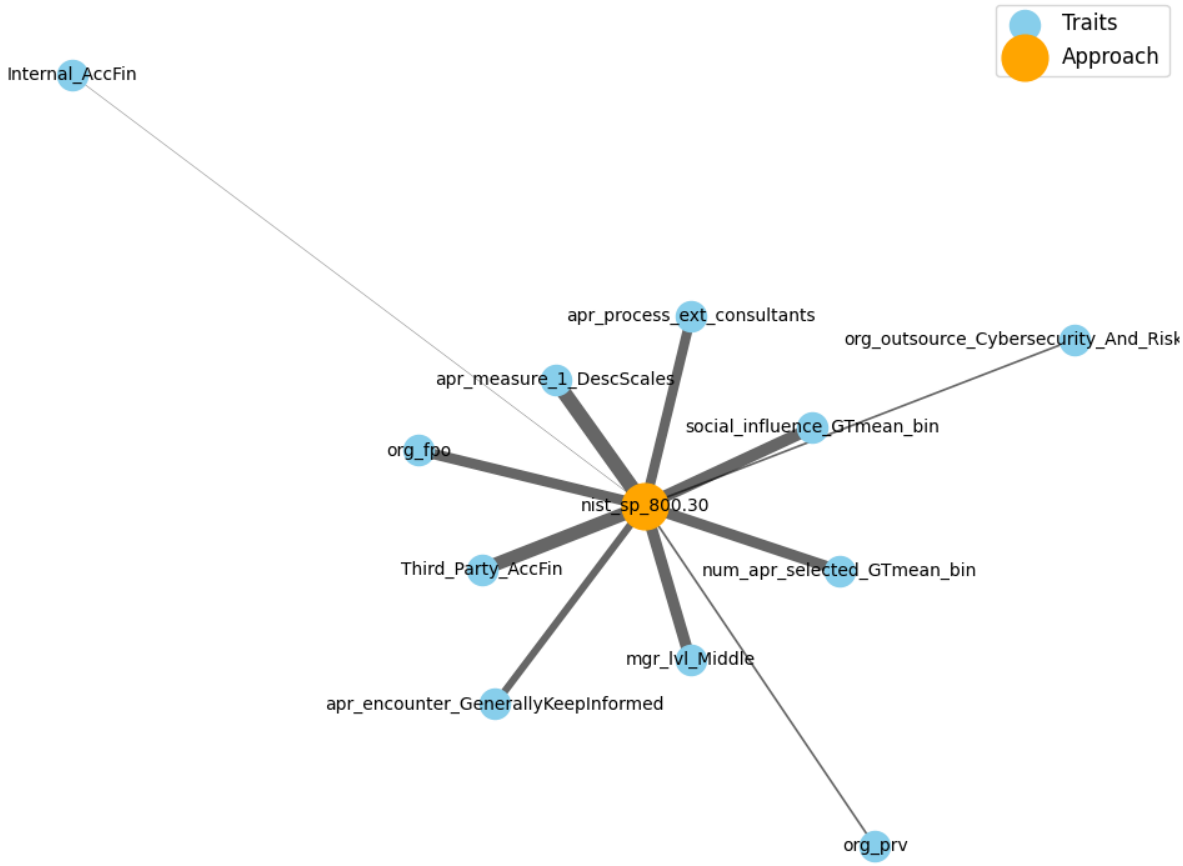


Figure 19

NIST SP 800-30 Approach and Top Traits by Frequency as Bipartite Ego Graph Network



Note: Edge lines thicken as trait frequency increases.

Based on Figure 18, the NIST SP 800-30 profile indicates a relatively concise set of prominent variables; however, none of them are substantially high compared to other approach charts. This suggests not having any high-standout traits. Yet, there are only a few predominantly important ones for this approach. Referring back to Table 36, the lift ranges associated with these traits suggest CSR managers with groups of these traits would be 4.32 to 21.60 times more likely to choose NIST SP 800-30 compared to someone who lacked these grouped traits. Notably, this profile is characterized by relatively higher grouping of CSR

managers who favor descriptive scales as a preferred risk measure, frequently work with third-party accounting and financial companies, and experience above-average social influence traits (as drawn from the TAM3 model).

When considered together, these traits may highlight selection patterns where social consensus and external validation are equally valued, possibly reflecting environments where the technical values for risk management adoption are optimized for group facilitation and external benchmarking rather than deep individual technical specialization. The moderate presence of middle management, using a more than average number of approaches, and for-profit status serve as additional key traits that further situate NIST SP 800-30 in organizations seeking accessible, business-aligned, and externally validated solutions.

Interesting, but not overly meaningful, the last bar in the figure pertains to the cybersecurity team working with internal accounting and finance groups, a converse trait to the external company version. This distinction could stem from those few organizations that have internal accounting and finance teams working with external counterparts, or simply offer a small nod toward the overall value organizations might place on participation from accounting and finance teams in general when it comes to CSRI&A.

5.3.5.5 NIST SP 800-37 RMF Association Rule Profile

Figure 20

NIST SP 800-37 Approach Profile - Most Freq Traits from Top 100 Association Rules by Lift

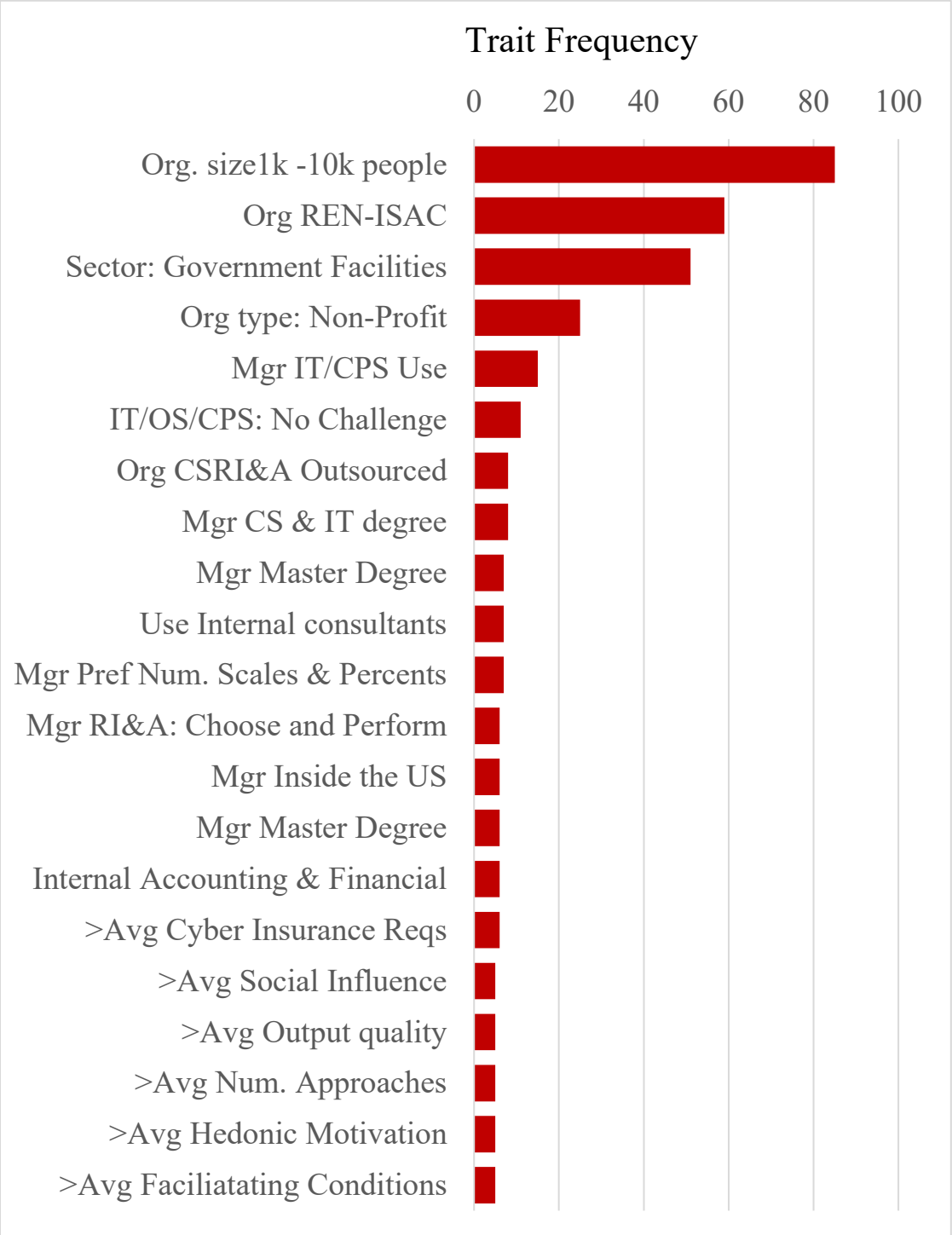
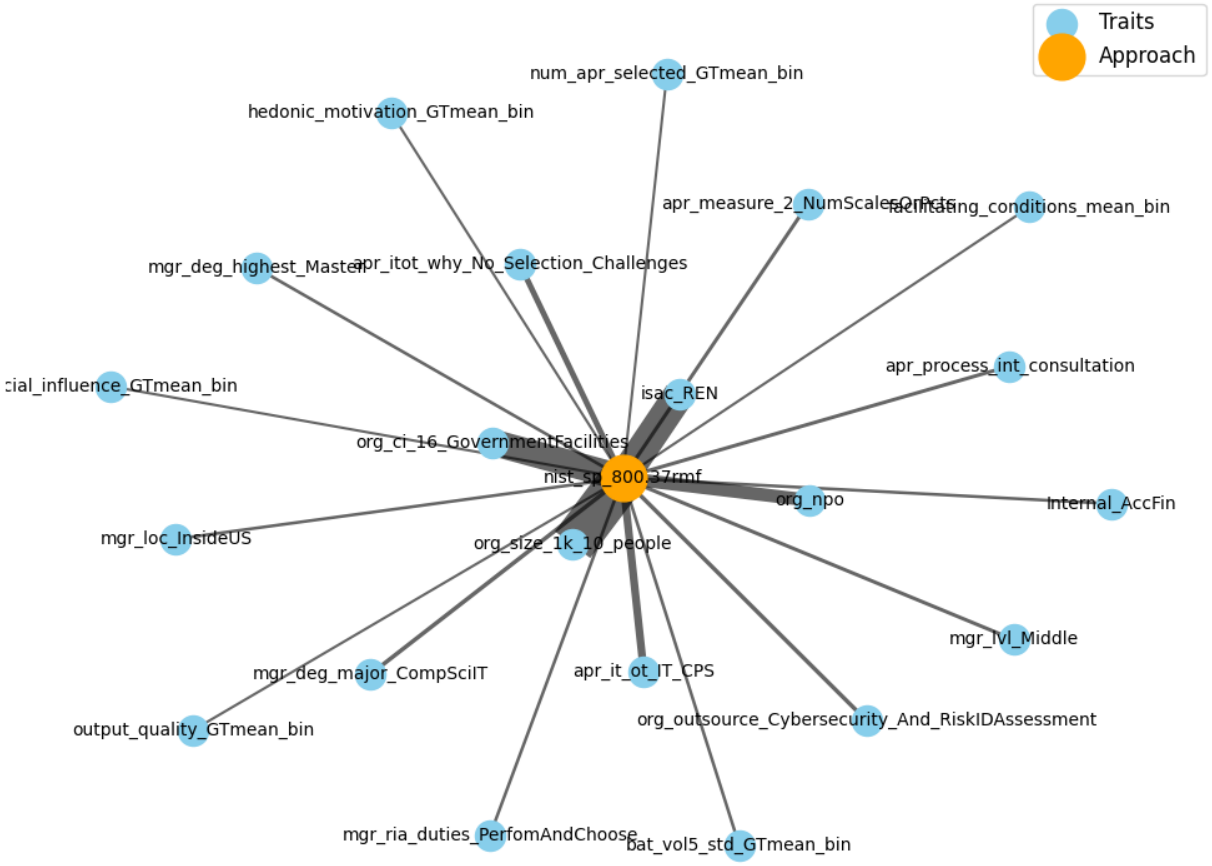


Figure 21

NIST SP 800-37 RMF Approach and Top Traits by Frequency as Bipartite Ego Graph Network



Note: Edge lines thicken as trait frequency increases.

Continuing with NIST, in the NIST SP 800-37 RMF Figure 18, the most prominent trait—organization size (1K-10K people)—is longer than any other, followed by a moderate trait group of the organization being part of the Research-Education ISAC, affiliation with government facilities critical infrastructure sector, and non-profit organizational types. These clustered bars, all hovering above moderate levels, suggest this approach is most closely associated with larger, institutionally complex environments, especially in the public and

nonprofit sectors. Beyond these traits, the others rapidly drop off and lack meaningful value-add to this profile. However, the large number of low bar traits suggests substantial variety among organizations that select the NIST SP 800-37 RMF. This is not surprising, given the NIST RMF is one of the widely known approaches outside the general 800 series, most of which lack their own popularized acronyms. Further reinforcing the organizational diversity of those selecting the NIST RMF, its lift ratios for the top 100 rules as all 10.29, meaning these traits all have the same association strength. Thus, it is likely the longer bars drive the selection, while any combination of lesser bar traits will tag along without meaningful impact.

5.3.5.6 ISO 27005 Association Rule Profile

Figure 22

ISO 27005 Approach Profile - Most Frequent Traits from Top 100 Association Rules by Lift

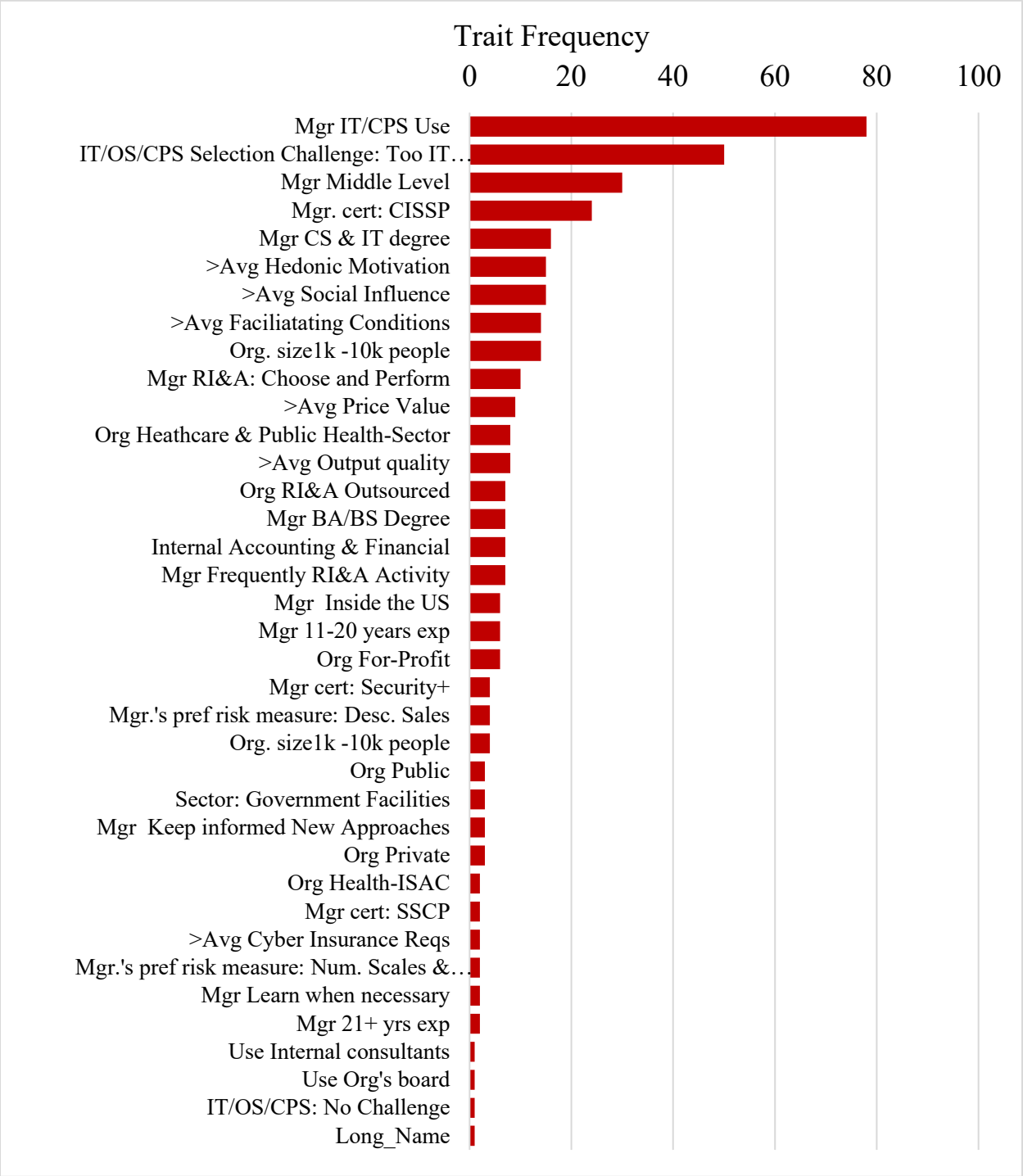
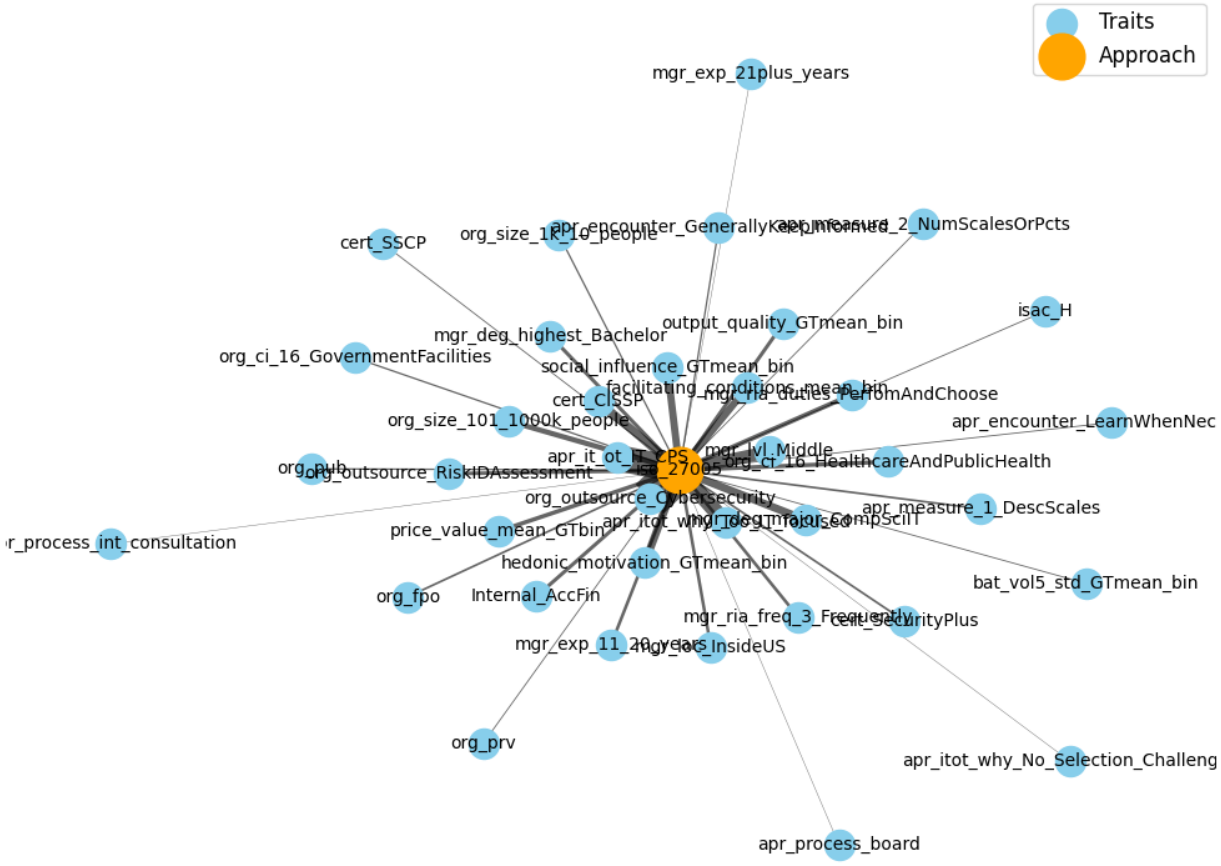


Figure 23

ISO 27005 Approach and Top Traits by Frequency as Bipartite Ego Graph Network



Note: Edge lines thicken as trait frequency increases.

The ISO 27005 chart, in Figure 22, features a sizeable number of traits but with a strong emphasis on just a few leading bars. The standout trait is the tendency for the organization to outsource its cybersecurity needs, followed next by the CSR manager use of the approach for IT and CPS assessment. Of particular note is the third bar, while 20 points lower, deals exclusively with CSR managers who believe most available approaches are too IT focused and not focused enough on a mix of IT, OT, and CPS uses. These three bars form the central profile theme of organizations concerned with technical proficiency and key cybersecurity needs, quite likely

with OT and CPS technologies. Interestingly, this approach is not specific to OT and CPS, but often used in reference to conduct information security risk assessments, typically in conjunction with ISO 27001 requirements.

5.3.5.7 Custom Approach Association Rule Profile

Figure 24

Custom / Bespoke approach (developed in-house and/or with third-party help)

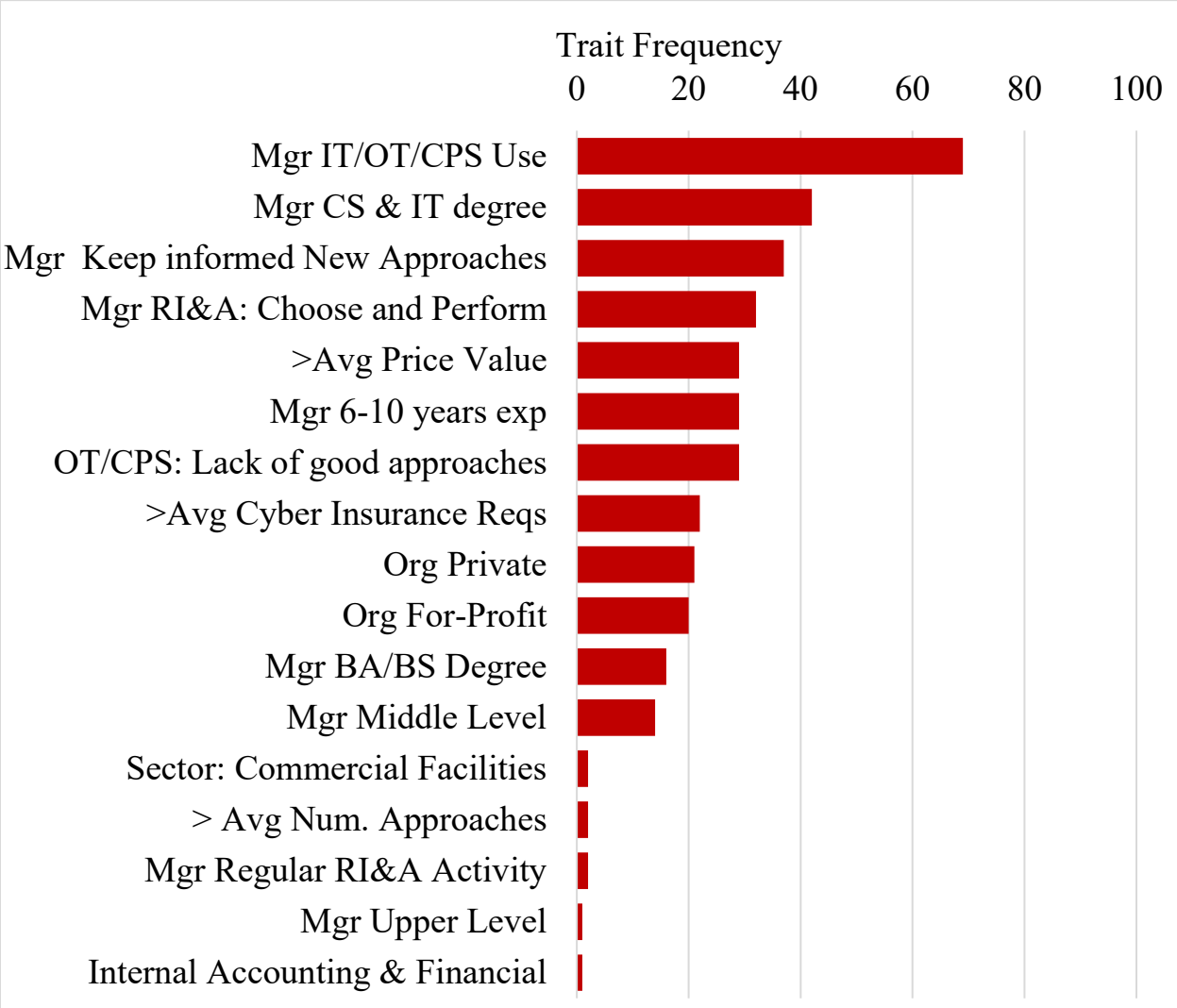
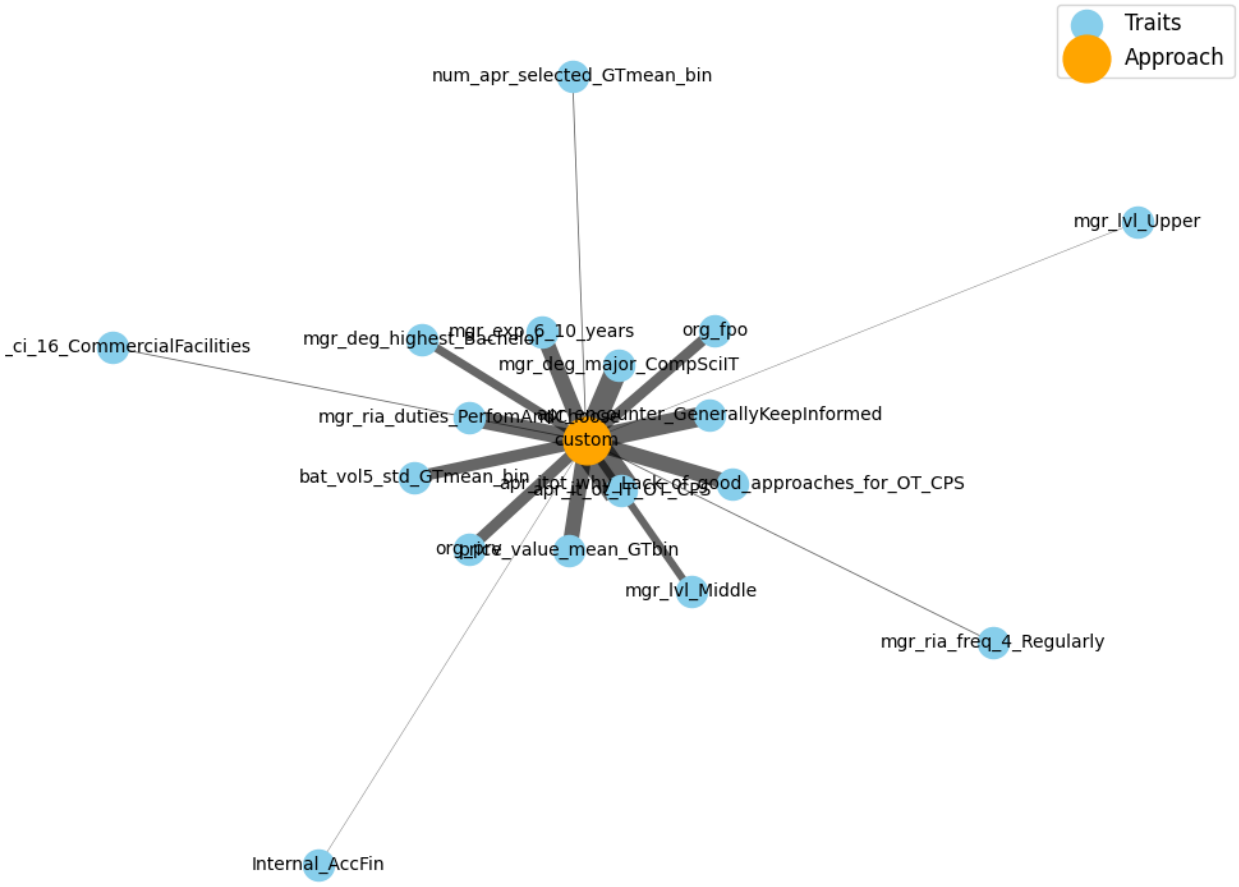


Figure 25

Custom / Bespoke Approach and Top Traits by Frequency as Bipartite Ego Graph Network



Note: Edge lines thicken as trait frequency increases.

The custom approach, shown in Figure 24 is distinctive for two reasons. First, it is not a singular approach in the way there is one NIST-800-30; rather, this custom approach is a catch-all for any form of bespoke, hybridized approaches, and so they could theoretically be developed to fit any managerial or organizational need. Selecting this approach is less about choosing one that is ready to go and more about the development and creation that goes into customization and bespoke options.

Notably, complete customization flexibility might initially suggest no association of common traits since you could build anything. Yet, the second distinction is that Figure 24 indeed shows one longer bar and several moderate bars before dropping off with smaller bar groups and then a few negligible traits. The predominant trait for custom approaches involves the CSR managers' use of IT, OT, and CPS needs. This echoes to both interview and survey findings that many approaches are insufficient for use in OT and CPS specific environments. That two of the profiles featured in this study are based on trait combinations pertain to OT and CPS needs is meaningful and warrants further investigation.

Notable frequencies of CSR managers for custom approaches are tech-types, often with computers science or IT degrees, who generally keep themselves well-informed of new approaches, and find regularly both choose and use their CSRI&A approaches. In other words, these CSR manager are technically savvy, hands-on individuals, who remain connected to cyber risk information sources. They are likely experienced, confident, well-resourced, and the type of manager that prefers development.

While this study did not explore many details about these custom approaches, it's likely these solutions are equally technical, hands-on, and connective if they are to meet the needs of this type of CSR manager.

5.3.5.8 Heatmap Micro Profiles from Aggregated Association Rules

With the initial profiles built for comparison, I also constructed a large cross-table with occurrence frequency of approaches in the columns and the managerial and organizational traits in the rows, it can be used to consider future profile building by observing trait distribution patterns, as well as relationships between traits and other approaches. The full Table 43 is in Appendix F, and in this subsection, I present a few key rows from that table to discuss a few

interesting patterns. Notably, this micro-dive discussion leans away from the multivariate analysis offered by the association rules charts above but allows for a cross-approach comparative. The table includes a heatmap color intensity when approaches match to a trait. Cells become darker red as the frequency increases and grey where the trait does not appear in that approach.

Table 37

Association Rules Traits - Approaches by Level of Management

Approaches / **Manager Level:**	Exec	Upper	Middle
CSC / CIS 18	2		
CMMC	18	14	1
CMMI	95		
COBIT			3
Custom		1	14
FAIR	68		
ISO-27001/2		1	2
ISO-27005			24
ISO-31000			29
MITRE ATT&CK	18	6	
MITRE Shield Engage			22
NIST CSF		6	3
NIST SP 800-171	11		10
NIST SP 800-30			22
NIST SP 800-37 (RMF)			7
NIST SP 800-39			9
NIST SP 800-53		8	
NIST SP 800-82		2	
NISTIR 8286			
OCTAVE			
PHA			14
SCF			22
SOC-C			1

Note: Values are trait frequencies in top 100 rules per approach. Grey cells have 0 value (empty).

Approach Pattern #1: Managers choose differently by level of management. (from *Table 37)*

Viewing Table 37, there is an immediate color shift between middle managers and executives with upper management straddling between the two groups. Some of these approaches offer more strategic level planning tools and facilitate organization-wide direction, such as CMMI, while MITRE Shield is very procedural and tactical in its usage, which makes sense for executive and middle manager groups respectively. Yet, there are others that buck this trend such as COBIT which is more process and high-level practice by favored by middle managers and not higher up. This warrants further investigation, both into approach details and multivariate data mining for related trait influence omitted here.

Approach Pattern #2:The type of accounting or finance team seems to matter with third party collaborators and AICPA familiarity having stronger preferences (from Table 38*)*.

Table 38 shows the most activity from CSR managers working with internal accounting and finance teams. In some cases, they leaned heavily toward approaches like NIST SP 900-171 and FAIR. In this case, internal generally meant fellow employees and not contractors or those in your network outside the organization. Once a manager connects with third party accounting and finance groups, approach selection changes drastically to options hardly used by internal teams, such as NIST SP 800-30, CMMC, MITRE Shield, and to a lesser extent, SOC-C. The last approach is of interest since SOC-C usually involves accounting firms to assess and attest to an organization's CSR management program. The low selection in this case could be due to managers not listing SOC-C if their organization did not need or was not interested in this reporting service. On the other hand, it is unclear as to why none of the managers familiar with the American Institute of Certified Public Accountants (AICPA), who offer SOC services, did not list the SOC-C. However, CIS 18 makes sense to appear with this group of traits given the

structured security control-based IG that leans heavily into inventory, audits, access controls and asset related management that would likely be familiar to accounting and finance groups.

Table 38

Association Rules Traits - Approaches by Accounting and Finance Teams

Approaches	**Org Cyberteam work group includes:**	3rd Party Acct & Fin	Internal Acct & Fin	Does not work with either	AICPA Familiarity
	CIS 18/ CSC	4	5	1	15
	CMMC	25	3		
	CMMI		16		
	COBIT		15		
	Custom		1		
	FAIR		26		
	ISO-27001/2		2	5	7
	ISO-27005		7		
	ISO-31000		14		
	MITRE ATT&CK		7		
	MITRE Shield Engage	25			
	NIST CSF		5	7	
	NIST SP 800-171		34		
	NIST SP 800-30	26	1		
	NIST SP 800-37 (RMF)		6		
	NIST SP 800-39	9			
	NIST SP 800-53		4		
	NIST SP 800-82		1		
	NISTIR 8286				
	OCTAVE		11		
	PHA		10		
	SCF		14		
	SOC-C	15	1		

Notes: Values are trait frequencies in top 100 rules per approach. Grey cells have 0 value (empty). “Acct & Fin” is shorthand for Accounting & Finance. AICPA is the American Institute of Certified Professional Accountants

Table 39

Approaches by Select Custom Approach Profile Traits

Approaches	CS / IT Degree Major	> Avg Price Value	> Avg Cyber Insurance Requirements	Lack of Good OT/CPS Approaches
CIS 18/ CSC	5	2	1	
CMMC	8	4	1	
CMMI				1
COBIT	5	5	5	
Custom	42	29	22	29
FAIR	11		4	
ISO-27001/2	6	5	4	
ISO-27005	15	8	2	
ISO-31000	0	1	13	
MITRE ATT&CK	15	2	5	1
MITRE Shield Engage		16		
NIST CSF	3	2	2	
NIST SP 800-171	5	4		
NIST SP 800-30				
NIST SP 800-37 (RMF)	8		6	
NIST SP 800-39		9		
NIST SP 800-53	4	2	4	
NIST SP 800-82		11	8	26
NISTIR 8286				
OCTAVE				
PHA	12	2	10	
SCF	3	19	5	
SOC-C	15		10	

Note: Values are trait frequencies in top 100 rules per approach. Grey cells have 0 value (empty).

Approach Pattern #3: Custom approaches still favor those that are likely to tinker and have specialized needs (Table 39).

This one is somewhat of an extension and reinforcement to the Custom approach profile discussion above. The four traits shared here all loaded into the Custom approach profile, but Table 39 adds the benefit of comparative highlighting with other approaches that draw upon those same traits. The custom approach, or rather any custom approach as there is not a singular version, is the only approach that draws seriously from these traits, with MITRE ATT&CK dabbling a bit. Lack of approaches useful for OT and CPS needs was a common concern with some of my interviewees [I19; I20] and is echoed here by survey participants. NIST 800-82 is an obvious choice for this group, since it pertains specifically to OT, while custom approaches allow managers to fill in CSRI&A need gaps. The other traits disperse broadly across the other approaches. Where it was unclear why those familiar with AICPA group above did not engage more with the SOC-C, the expectation is met here by viewing managers with greater than average cyber insurance coverage needs to acquire that attestation. Computer science and IT degree trait load onto approaches that seem more friendly to tinker types, but all other choices are few below their custom approach selection. Interestingly, managers with the higher-than-average price value preferences chose very few NIST products. There was some loading onto a couple NIST approaches, but not a wide adoption. Instead, there was greater spread with other approaches that would cost much more than the free NIST price tag. Yet, this table does not show which counts come from managers choosing more than one approach, which is often the case with the 2.7 approach average among the survey respondents.

These micro-reviews serve as a useful balance check with the individual profiles, viewing traits across multiple approaches as a counterbalance to the singular approach focus of the

profiles. As more work is done on profile development, returning to the wider view heatmap trait and approach comparison tables will help illustrate where traits flagged as meaningful for an approach profile can be viewed in the larger context across approaches and inform a broader profile narrative.

5.3.5.8 Next Steps with Association Profiles

Synthesizing these findings, establishing profiles through association rules is a novel method for visualizing and classifying CSR managers. The selection patterns and profile characteristics suggest a mutual alignment based on managerial and organizational traits, shaped by professional background, organizational structure, and external influences. The most significant traits for each approach are consistent within each profile and sharply differentiated from one another, indicating that approach selection is not random; rather, it is closely tied to the specific needs and characteristics of the adopting organization. Additionally, these profiles are not mutually exclusive, meaning they may align with more than one approach. Further work is needed to develop quiz-type assessments that match managers with profiles while exploring connections to approaches.

Access to this material is currently limited to me as part of this study. Once available in the future, cybersecurity professionals may find practical value in using the profiles as a data-driven way to benchmark their organizations or clients against the most common adopters of each approach. For organizations, these profiles act as mirrors, helping CSR managers, their teams, and stakeholders evaluate whether their current selection of approaches aligns with the traits most strongly associated with sustained and effective use. For instance, an organization led by highly experienced executives in a growth-driven, for-profit environment may find that FAIR aligns naturally with its needs, while organizations with more diverse managerial profiles may

consider broader standards like ISO 27001 a better fit. Understanding the "who" behind typical approach adopters allows CSR managers to benchmark themselves against their professional peers and assess whether they share the same strengths or if complementary adjustments are needed. Thus, profiles become tools for self-assessment, indicating where a chosen approach may integrate seamlessly with organizational practices or where vulnerabilities in adoption could arise.

These findings also highlight the importance of flexibility and adaptation in approach design and adoption. Some standards, like FAIR, yield clear and consistent profiles around executive decision-making in experienced, for-profit environments, making them narrow yet highly targeted. Others, such as ISO or CIS18, connect with a more diffuse set of managerial and organizational traits, creating opportunities for wider but less predictable adoption. For organizations, these distinctions clarify whether to commit deeply to an approach that aligns with their leadership identity or to adopt broader frameworks that can adapt to diverse internal needs. In both cases, profiles add predictive insight, helping practitioners anticipate not only the technical requirements of a framework but also its cultural, financial, and managerial fit. For consultants, this means profiles can indicate whether an approach should be framed as specialized or generalist when advising clients.

Consultants could also leverage these insights to design bespoke solutions that align with their clients' unique traits, while organizations can use the profiles to assess whether their current practices align with those most likely to succeed. This targeted understanding can help reduce the risk of approach abandonment, improve alignment with organizational goals, and support more effective resource allocation.

By examining association rules and developing persona profiles, I've identified patterns and key factors behind how managers select cybersecurity approaches. These insights help explain the decision-making process in real-world organizations. With this foundation, the following conclusion chapter highlights the main findings and discusses their implications for practice and future research.

Chapter 6: Conclusion

The previous chapters revealed a clear range of cybersecurity risk identification and assessment approaches selected and used by cybersecurity risk managers. It also showcased the factors influencing approach selection, highlighting the interplay between individual and organizational preferences, measurement practices, sector-specific influences, and the application of a novel selection framework. Having addressed the multifaceted choices and trade-offs managers face, this final chapter synthesizes these empirical insights and their implications, connecting the motivations established in Chapter 1 to the inquiry. I will also summarize the contributions to both scholarship and practice, acknowledge study limitations, and propose clear directions for future research and professional advancement.

6.1. Summary of Research Study

While studying cybersecurity management, policy, and governance, I identified a keystone issue within critical infrastructure cybersecurity. Grouped into 16 CISA-defined sectors, organizations across the US—including water treatment plants, Wall Street, communication stations, and chemical plants—rely on leadership to determine CSR management, including choices regarding CSRI&A. These choices are crucial, as they set the initial risk decisions that could lead to cyber disruptions ranging from power loss and economic harm to threats to public safety, compounded by the rise of cyberattacks on critical infrastructure. Complicating this decision space is a complex and dynamic marketplace of I&A approaches, each originating from various public, private, and academic sources. This variety of supply-side options presents significant challenges for CSR managers seeking to select the most effective strategies for their unique organizational environments.

This decision landscape motivated my work, which began with two central questions: what do CSRI&A approaches managers choose (RQ1), and why do they choose those approaches (RQ2)? Understanding the approaches CSR managers select reveals insights into operational strengths and challenges based on approach features, as well as market competition and dominance among approaches. This understanding is essential for improving strategic fit and effectiveness in complex environments. This dissertation thus seeks not only to map current practices but also to uncover the deeper mechanisms of managerial decision-making that drive framework selection (or rejection).

From a methodological standpoint, I employed a two-phase design. The first phase involved 22 semi-structured interviews with high-level cybersecurity managers—individuals with significant discretion and responsibility in their organizations. These interviews developed a grounded understanding of selection preferences and contextual influences. The second phase included a broader survey of 216 mid-to-high-level managers, designed to validate and enrich the interview findings by aggregating self-reported behaviors, perceptions of alternatives, and organizational fit considerations.

I developed a novel conceptual framework based on literature across several scholarly domains, rooted in a cybersecurity context. The framework draws from technology adoption theory, decision-making research, and information behavior models, intentionally designed to analyze not just the approaches themselves but the interplay of knowledge, organizational culture, and external policy influences that shape approach compatibility. The interviews confirmed the framework's initial usefulness and informed the development of survey questions to further assess its application potential. By situating CSRI&A methodology within actual

managerial contexts—where discretion is constrained by both internal policies and external standards, recommendations can be meaningfully tailored for improved cybersecurity practice.

Beyond the framework, the rich interview and survey data provided additional emergent topics discussed in Chapter 5, which substantially extended and enriched the study's original scope. These findings revealed nuanced dimensions—such as the influence of consultant engagement, evolving preferences for quantitative risk metric specificity, and sector-specific drivers for framework adoption—that were not anticipated at the outset but emerged as critical factors shaping organizational cybersecurity risk identification and assessment practices. Additionally, this work introduced the innovative application of association rules as a data mining technique to explore and map multivariate associations across managerial roles, organizational traits, and decision contexts. This computationally informed process surfaced patterns and perspectives that provided essential context for my dissertation's contributions, highlighting both the diversity and sophistication present in real-world decision-making.

6.2. Summary of Major Findings

The study's major findings reveal a landscape of exceptional diversity in risk identification and assessment approaches among cybersecurity managers, reflecting the wide array of organizational contexts and the evolving nature of the cybersecurity domain. Analysis of interview and survey data demonstrated that managers actively employ a variety of models—such as NIST SP 800-53, CIS Controls, ISO 27001/27002, COBIT, and in-house hybrid approaches—with roughly 60% of interviewees reporting the use of multiple approaches and an average of 2.7 approaches selected per survey respondent. This plurality signals the need for customization to unique organizational needs and recognizes that no single framework fully

addresses the multitude of sector-specific risks and internal practices encountered across critical infrastructure sectors.

The findings also highlighted the strong interplay between regulatory mandates, organizational context, and framework adoption. Government requirements often acted as primary drivers for the selection of NIST-based standards, particularly in organizations with federal ties or public utility status, while private-sector managers frequently leveraged ISO standards to support international operations or to align with global partners. The survey further revealed that many organizations blend mandated and voluntary frameworks, adjusting their implementations to fit resource constraints, sector pressures, and compliance reporting needs. This blend led to a spectrum of framework loyalty, from strict adherence to ad hoc hybridization, depending on the regulatory environment and internal business drivers.

This prompted exploration of compatibility and ongoing conflicts between widely used families like NIST and ISO. While both frameworks are regarded as robust and reputable, several participants described challenges in achieving seamless integration: overlapping requirements can cause process duplication, while differing emphases (such as the prescriptive controls of NIST versus the management system focus of ISO) present organizational challenges. Social factors emerged as influential determinants of approach selection, framework loyalty, and hybridization. Trust in framework efficacy—shaped by peer endorsements, consultant recommendations, or prior personal success—often outweighed purely technical criteria in decisions to maintain or switch approaches. Manager participation in professional associations and ISACs facilitated framework learning and spread, while the costs associated with rigorous implementation, especially in smaller organizations, were cited as barriers to both adoption and long-term adherence. These social dimensions created opportunities for bespoke approaches,

particularly when leaders needed to reconcile cost, workforce capacity, and the desire for consistent risk language across organizational boundaries.

This study revealed substantial differences in the use and perceived value of quantitative measurement practices for risk communication. While some managers strongly advocated for strict numeric scoring to enhance accountability, support executive decision-making, and meet compliance needs, others expressed skepticism regarding the reliability or interpretability of quantitative methods, especially when underlying data were sparse or subjective. Preferences often leaned toward less quantitatively rigorous measurements, such as one IT senior director's use of heatmaps for the Board to improve CSR communications [I22] or a health executive mentioning that heatmaps are "easy," albeit "wildly inaccurate" [I17]. This variability has clear implications: inconsistent measurement practices can hinder internal communication, foster misunderstandings among stakeholders, and complicate cross-organizational collaboration, suggesting a continued need for guidance around the calibration and integration of quantitative risk metrics in practice.

6.3. Contributions and Implications

This section identifies the central contributions and implications of the study, linking the major findings to both theoretical advancement and practical CSR management. From the preceding summary, the discussion now moves to articulate how these outcomes build on scholarship and may influence the broader academic field. These contributions set the stage for the following analysis of practical implications.

6.3.1 Scholarly Contributions

Within the broader contributions, my research seeks to help advance scholarly research on several fronts. This subsection details how the study adds to existing literature, offers new

perspectives on well-established theories, and shares novel findings with the field. These academic insights complement the forthcoming review of practical applications and limitations.

6.3.1.1 Theoretical

From a theoretical perspective, the conceptual framework developed in this study integrates multiple well-established theories relevant to cybersecurity decision-making, bridging individual, organizational, and technical aspects. Instead of advancing each foundational theory of diffusion, decision choice, user acceptance, and organizational structure separately, this framework synthesizes their complementary explanatory capabilities into three operationalized constructs: fundamental understanding differences, functional differences, and situational differences. This synthesis addresses a gap in CSR management research, where existing single-theory approaches capture only partial explanations of complex managerial decision-making processes (Figure 2).

The framework's theoretical novelty lies in its ability to systematically examine approach selection through a more comprehensive analytical lens than each contributing decision theory could offer. One insight is the identification and exploration of bespoke approaches where organizations blend elements from multiple standards—most notably NIST and ISO—to tailor risk identification and assessment approaches that better fit their unique contexts. This concept challenges traditional theories of technology adoption, which focus on adoption, acceptance, strategy choice, fit, use, abandonment, and replacement (Tarhini et al., 2015; Campagna & Bhada, 2024; Yadegari, Mohammadi, and Masoumi, 2024), by shifting attention from singular technologies, such as CSRI&A approaches, to multiple amalgamations into something new. This underscores the dynamic, adaptive nature of cybersecurity governance in practice. The research also clarifies the nuanced compatibility and conflict between NIST and ISO standards,

demonstrating how overlapping requirements and differing emphases create both opportunities for synergy and challenges for integration.

Within the framework, multi-construct decision-making patterns provided several insights about cybersecurity approach selection. First, they explained why approach selection often seemed irrational when viewed through single-construct lenses. Managers who chose technically inferior approaches were often making sophisticated multi-dimensional decisions that balanced competing demands across all three constructs. Second, multi-construct patterns revealed why approach implementation success varied dramatically across organizations. Approaches that aligned well across all three constructs showed higher implementation success and lower abandonment rates. Conversely, approaches selected based on single-construct reasoning often faced implementation challenges when conflicting pressures arose from other constructs. Third, the multi-construct framework explained why recommendations from best-practice studies often failed in specific organizational contexts. Recommendations typically focused on functional effectiveness while ignoring fundamental understanding gaps or situational constraints that complicated implementation.

In addition to the conceptual framework, this research contributes to the theoretical understanding of cybersecurity management in critical infrastructure by enhancing the academic discussion of RI&A decision-making processes in complex organizational environments, from people to structures. For instance, Setiawan et al. (2025) noted that organizations treating cybersecurity as a separate technology from other enterprise functions compromise their ability to identify threats clearly and respond effectively to incidents. In contrast, incorporating security considerations into a comprehensive, cross-disciplinary organizational risk management strategy

enables proactive threat detection, systematic vulnerability ranking, and strategic threat reduction.

This study focuses on high-level managers, from senior managers to the C-suite, placing CSRI&A decision-making and outcomes in the same spaces where those managers may choose to integrate their CSR activities across departments and functional areas. The high-level managerial focus also allows their CSR planning actions to consider the regulatory environment and external stakeholder conditions. This research builds on Tisdale (2016), who used a systems approach to navigate CSR management factors and their interrelationships, by empirically demonstrating how cybersecurity risk management is shaped not only by systems-level interrelationships but also by the dynamic selection and hybridization of frameworks in response to organizational context and leadership priorities. Extending Ogbanufe et al. (2021) regarding institutional pressures on top management for CSR resource commitments, my findings show that institutional pressures and top management values influence not just resource commitments like cyber insurance but also the adoption and adaptation of risk management approaches, including the blending of standards such as NIST and ISO. Both Tisdale and Ogbanufe et al. may be interested in citing my work for its evidence that managerial decision-making in cybersecurity is a multidimensional process, where leadership, institutional forces, and technical frameworks interact to produce tailored, context-sensitive strategies for risk mitigation.

This work is timely, coinciding with the rise of generative AI and agentic AI swaying the public zeitgeist and influencing research. While this research does not directly explore AI-made, based, or assisted approach selection, the deep exploration of the CSR manager's human and organizational traits serves as a cross-section for comparison to future AI-related CSR decision-making research. For example, Kush (2025) discussed a "human-machine identity blur"—a

"convergence point where human and machine identities overlap, delegate authority, and create novel attack vectors." In such a decision system, algorithms could automate the selection of CSRI&A approaches, although how 'good' or 'successful' automated selections turn out is uncertain. As this study shows, there are a wide range of approaches and selection factors, including situational context that can be challenging for algorithmic decision-making to grasp in isolation.

Computerized systems already exist to collect metrics and data used in CSRI&A activities, functions that in some organizations are still monitored and collected by humans. It is not a far leap to envision how senior managers could offload CSRI&A decisions and duties to an automated system. In such cases, this research aids in comparing how selected approaches may differ over time, as well as related decision-trait variations. Altogether, this work may inform the adaptation of current and the development of new theories on AI-assisted executive leadership. Powell (2025) discussed such changes with his CISO 3.0, where new technologies, such as ChatGPT, further shift the technological and business landscape. Meanwhile, Dotan et al. (2024) detailed issues of trust, consensus building, and other sociotechnical harms related to the development and implementation of AI principles, suggesting that NIST's relatively new AI RMF could be a potential solution to these challenges.

6.3.1.2 Empirical

Ultimately, RI&A choices made by the CSR manager are critical as they affect the safety and security of not only the manager's organization but also the social and commercial actors that rely on the critical infrastructure services provided by the organization. The CSR manager is a key factor in the local and broader economies. Thus, the empirical findings in this study

provide insights into the CSR manager's risk-related mindset, decisions, and information environment.

This study represents a first known effort to directly ask CSR managers in critical infrastructure organizations what approaches they use and why through interviews and a survey. Additionally, participants shared whether the approaches they use for their CSRI&A duties are sufficient and which approaches they abandoned. While well-known approaches from ISO and NIST were frequently mentioned, this study also included lesser-known and niche approaches like the functionally specific SOC-C and sector-specific NERC CIP.

Recent work by Gilbert & Gilbert (2024) in the energy, transportation, and healthcare sectors suggested integrating various frameworks to balance cyber risk management activities and addressing emerging technology challenges, including IoT and AI. This study supports CSR managers, as using multiple approaches simultaneously was common; over 75% of the survey participants reported using more than one approach.

Multiple choices for approach selection also lean toward custom approaches. CSR managers turned to bespoke approaches to achieve specific results that fit their organizations. In this niche area, manager contexts vary. One manager focused on "information system and compliance needs" [S60], while another combined needs from "security/risk teams and the National Infrastructure Protection Plan" [S91]. Individual factors matter as well, with one manager's selection influenced by internal "high-level execs" and "departments" [S100], and another's selection reflecting "relationships with key business stakeholders, C-Suite, and IT" [S111].[35] While the total number of managers using bespoke approaches was too small to

[35] Manager details moved to footnote for readability. S60: middle manager in a private, for-profit telecommunications sector organization; S91: middle manager in a public, non-profit water and wastewater sector organization; S100 and S11 are upper-level managers in private, for-profit commercial

establish recurrent patterns, their overall presence opens avenues for further exploration in this area of dynamic approach choice.

This study unexpectedly identified the use of consultants as a key theme in the approach selection process. The literature on cybersecurity management consulting is extensive, with resources such as Refsdal et al. (2015) on cyber risk, Hubbard (2016) on risk management, and Hubbard & Seiersen (2016) on measuring cyber risk providing foundational knowledge for the cybersecurity consulting industry. Meanwhile, newer works in cyber management consulting explore specific areas, such as agency theory perspectives that may influence cyber risk governance and conflicts of interest (Burch et al., 2024). However, none addressed the role of consultants in approach selection. This study aims to motivate a subtopic of research that could support a special journal issue or conference.

Like the consultants, this study's research design did not explicitly intend to assess approach abandonment. While numerous studies have explored the intersection of technology adoption and abandonment, research in the CSRI&A context is limited. Recent work in CSRI&A technology abandonment focuses on areas such as machine learning and AI (Mun & Housel, 2023), resource management (Ahvari, 2023), or specialized topics like employee reactions during vulnerability assessments (Pienta et al., 2024). Therefore, while evidence from this study is limited, it contributes to the unexpected practice-research gap in approach abandonment.

Whether using internal or external consultants or making decisions independently, CSR managers consider measurement preferences in their approach choices. Evidence from this study revealed a divide between instructional texts like Hubbard and Seiersen (2016), which advocate

---

facilities sector organizations. All reported being involved in both choosing and performing the approaches they selected.

numeric risk metrics, and the aggregate preferences of CSR managers for rank-order scales. The absence of a second-round survey limited the exploration of this finding; however, variations in risk measurement preference were reported based on critical infrastructure sector, level of CSR management, and the way CSR managers encountered new approaches. This variability has meaningful implications for risk communication, accountability, and cross-organizational collaboration, highlighting the need for flexible yet coherent measurement strategies that balance precision, cost, and interpretability.

A methodological contribution of this dissertation lies in applying association rule mining to develop empirically grounded selection profiles for CSRI&A approaches. By leveraging association rules analysis on a rich dataset of managerial and organizational traits, I uncovered complex, multivariate patterns that extend beyond simple bivariate or trivariate patterns or the limited interaction structures typically modeled through regression techniques. Methodologically, this research also borrows from marketing research and data science, particularly through a novel application of association rule mining and bipartite graph network analysis. These graph-based structures facilitated a visual and relational understanding of how CSRI&A managerial choices cluster with other factors, such as organizational affiliations, demographics, and individual preferences, revealing the interconnected nature of managerial decision ecosystems.

These combined data mining and graph-analytic approaches demonstrated that the likelihood of selecting a framework like FAIR dramatically increases when specific traits—such as executive-level management, over 21 years of experience, and a for-profit organizational context—co-occur, with lift values indicating a significantly higher probability of selection compared to managers lacking those traits. The resulting selection profiles provided a nuanced,

data-driven understanding of which combinations of professional background, organizational structure, and operational practices are most strongly associated with adopting specific frameworks. The use of graph models, while common in cybersecurity for modeling networked threat environments, is newly applied here to managerial decision structures in CSRI&A, offering a fresh lens for visualizing how managerial traits and framework choices converge. In practical terms, these empirically derived profiles and visualizations could assist cybersecurity professionals in benchmarking and refining their own or clients' approach-selection processes or identifying traits conducive to forming bespoke approaches. For scholars, my study demonstrates the potential of data-mining techniques to explore the hidden structures of cybersecurity managerial decision-making in complex socio-technical domains, offering a data-informed, descriptive pathway between longstanding qualitative traditions and generalized, quantitative inferential models. In summary, the integration of association rules, graph network modeling, and profile development represents a methodological innovation that both deepens and diversifies the empirical tools available for cybersecurity management research. Collectively, these contributions enhance understanding of the drivers behind framework adoption and hybridization in CSRI&A approaches while bridging the methodological gap between qualitative insights and quantitative rigor in cybersecurity risk management research.

6.3.2 Practical Implications

This research provides actionable insights for practitioners responsible for CSRI&A in critical infrastructure and beyond. First, the study confirms that managers routinely draw from a diverse mix of frameworks—such as NIST, ISO, CIS Controls, and custom hybrids—rather than relying on a single standard. This diversity reflects the need to tailor risk management strategies to specific organizational contexts, regulatory requirements, and available resources. For

practitioners, this means that benchmarking against peers or industry norms should account for the reality of multi-framework environments and the value of custom hybrid approaches that combine strengths from multiple sources.

Regulatory mandates remain a powerful driver of framework selection, often overriding personal or technical preferences. Organizations subject to federal or sector-specific regulations will likely need to prioritize compliance with NIST or similar standards, while those operating internationally may find ISO frameworks more compatible with global partners. However, the research shows that many organizations blend mandated and voluntary frameworks, adapting them to fit their unique needs. Practitioners should be prepared to navigate these regulatory pressures and consider how to harmonize overlapping requirements to avoid duplication and inefficiency.

The findings indicate that effective CSR management must accommodate both mandatory standards and voluntary adaptations, highlighting a need for ongoing dialogue between organizational leaders and regulatory agencies. As agencies such as CISA and NIST update guidelines and sector-specific requirements, integrating real-world evidence from managerial practice can help ensure policy relevance, support sector-wide alignment, and promote pragmatic cross-sector collaboration.

Compatibility and conflict between major standards—especially NIST and ISO—are common challenges. Managers reported that while both frameworks are robust, integrating them can lead to process redundancy or confusion due to differing emphases (e.g., technical controls vs. management systems). Practitioners should note the importance of mapping requirements carefully and engaging stakeholders across departments to ensure smooth implementation and sustained use.

Social factors such as trust in a framework, participation in professional associations, and cost considerations significantly shape approach selection and loyalty. Trust is often built through peer recommendations, consultant input, and positive past experiences, while cost and resource constraints can limit the feasibility of adopting or maintaining certain frameworks. Practitioners should foster a culture of collaboration and continuous learning, leveraging both internal and external expertise to inform decision-making and support framework adoption. Quantitative measurement practices vary widely, with some managers favoring detailed risk scoring while others rely on ordinal scales. This variability can impact risk communication, especially when translating technical findings for executive or cross-departmental audiences. Practitioners should assess their organization's measurement preferences and capabilities, aiming for a balance between precision and interpretability that supports clear, actionable risk reporting.

The use of association rules and the development of selection profiles provide practical tools for understanding which combinations of managerial and organizational traits are most strongly associated with adopting specific frameworks. For example, the likelihood of selecting FAIR increases dramatically for executive-level managers with extensive experience in for-profit organizations. These profiles can help practitioners benchmark their own approach selection processes and identify other approaches that may better align with their needs. By applying data-driven insights to framework selection and adaptation, cybersecurity managers can make more informed, context-sensitive decisions that enhance organizational resilience and risk management effectiveness.

6.4. Limitations of the Study

This study's findings should be viewed in light of several important limitations. First, my overall sample size was not large, comprising 22 interviews and 216 surveys. While these sample

sizes are adequate for initial exploratory data analysis and evaluating my framework and association rules, I remain cautious about external validity and replicability due to the unbalanced subgroup sizes. Additionally, sector representation posed constraints: although this research included various managerial roles and organizational types, critical infrastructure sectors—such as dams and nuclear—were underrepresented. Conversely, when I had a larger group of participants by sector, the proportions of top sector subgroups varied significantly between the interview and survey samples.[36] This may limit the applicability of results to specific sectors, especially when regulatory environments and risk profiles differ across sectors or operational activities.

Second, reliance on self-reported data and interview-based methods introduces potential biases. Ideally, I would collect real-time observational decision data; however, many CSR details could involve sensitive information that made it extremely challenging to recruit study participants post-decision and rendered real-time decision participants inaccessible.[37] Thus, my post-decision participants may have described their decision-making processes in ways that reflect social desirability, recall bias, or post-hoc rationalization, rather than offering a fully accurate account of their actual practices. These biases can affect the reliability of insights into framework selection, organizational adaptation, and risk communication. This is particularly acute with the survey, where I was unable to immediately follow up with probing questions to clarify the survey's open-response questions or target other questions based on respondent characteristics.

---

[36] My top interview sectors were IT and Government Facilities (23% each), and the Defense Industrial Base (DIB; 16%), compared to Commercial Facilities (18%), Critical Manufacturing (14%), and Healthcare & Public Health (12%). Refer back to Table 23 in Chapter 5 for the sector distributions.
[37] I posit that without special contacts and permissions, no researcher would not be able to obtain direct observational data, as this type of secure information is not something open to outsiders.

Third, the generalizability of the study is limited by the rapidly evolving nature of the cybersecurity landscape and the continual emergence of new frameworks and technologies. The cross-sectional design provides a single snapshot of current practices but may not capture how approach selection and implementation shift in response to new threats, regulatory changes, or innovative methodologies. In particular, the emergence of generative AI has already transformed many industries and areas of operations. My general understanding of CSR managers leans toward a skeptical or conservative view on technologies, such as generative AI or agentic AI, that reduce agency in core decisions. However, a recent ISC^2 (2025) report indicates significant AI adoption within cybersecurity operations. Therefore, findings should be interpreted as representative of the current context, with the understanding that future developments may alter the patterns and reasoning observed in this research.

6.5. Directions for Future Research

Building on the findings and limitations of this study, several promising avenues for future research in CSRI&A emerge. First, expanding the sample size and sector representation—especially in underrepresented areas such as dams, nuclear, and possibly non-US regions—would help validate and generalize the observed patterns of framework selection and adaptation. Comparative studies across different sectors and contextual environments could illuminate how geographic and policy contexts shape CSRI&A practices and decision-making.

Second, future research could consider longitudinal study designs to capture how approach selection and implementation evolve over time in response to changing threats, organizational learning, and leadership transitions. For example, my survey could be refined and conducted annually with better sampling quotas for critical infrastructure sectors and subsectors. An annual survey would complement the local government cybersecurity surveys by Norris and

his team at the UMBC Cybersecurity Institute (Norris, 2025), since many local government operations are part of critical infrastructure and help provide context for why many "fail to manage cybersecurity well" (Norris et al., 2021). For the broader practitioner community, my survey could enhance major annual cybersecurity surveys and research reports, such as ISACA's State of Cybersecurity (ISACA, 2025), Cisco's Cyber Threat Trends report (Cisco, 2025), or Gartner's Top Cybersecurity Trends (Gartner, 2025) by connecting findings from those reports to deeper insights from my survey regarding the dynamics of framework adoption, abandonment, and hybridization, as well as the impact of emerging technologies and innovative risk management methodologies.

Third, the study's use of association rules and profile development opens the door for advanced data mining and machine learning techniques to uncover complex, multivariate patterns in approach selection. Future work could refine these methods to predict framework adoption, identify best-fit profiles for specific organizational contexts, and support more personalized guidance for cybersecurity managers.

Fourth, this study would benefit from considering the role of AI, including generative AI and agentic models, in the approach selection process. According to the 2025 AI Pulse Survey from ISC^2 (2025), 30% of cybersecurity teams have "already integrated AI security tools," and 42% are "in the test/evaluation stage with plans to integrate," while only 10% have no plans to start. Generative AI and agentic AI were part of ISC^2's AI survey definition. That same report noted that 36% of respondents believed governance, risk, and compliance was an area in which security operations would be most impacted by AI security tools (ibid).[38] As generative AI

[38] Governance, risk, and compliance ranked in the middle of 12 security operations categories, with agreement percentages ranging from 20% to 60%, excluding the Other and Don't know categories.

models become increasingly sophisticated, they offer new opportunities for automating the synthesis of threat intelligence, generating tailored risk scenarios, and supporting decision-making through dynamic framework recommendations. It is plausible AI may be adopted for such tasks as defensive strategies to keep up with AI-based attack tools as well. Such use of AI could lead to new approaches that capture AI use. Additionally, AI may become more involved as a decision aid among leadership, thereby affecting approach selection. Moreover, examining the ethical, transparency, and trust implications of deploying generative AI in critical infrastructure contexts would be essential to ensure responsible adoption and alignment with organizational, managerial, and regulatory standards.

Finally, as the cybersecurity landscape continues to evolve, ongoing research should track the emergence and integration of new frameworks, measurement tools, and socio-technical factors. This includes exploring how organizations balance quantitative and qualitative risk metrics, adapt to regulatory changes, and foster collaborative, trust-based cultures for effective risk management.

Relatedly, I would also like to see more work done that explores the managerial decision space illustrated in Chapter 3 and how it influences management decision-making. Work in this expansion area should examine the macro-level impacts of managerial and organizational approach selection, particularly as cross-sector interdependencies, supply chain vulnerabilities, and international standards harmonization challenge existing models. By mapping how micro and meso-level decisions contribute to systemic risk or resilience, scholars and practitioners can inform policy responses that better address the complexity of national and global cyber threats. By addressing these areas, future studies can further strengthen both the theoretical and practical foundations of CSR management.

6.6. Closing Reflection

This dissertation aimed to illuminate the complex, dynamic landscape of cybersecurity risk identification and assessment, focusing on how managers navigate a crowded field of frameworks, regulatory pressures, and organizational realities. Through a combination of research methods, the study revealed that effective risk management is not simply a matter of technical compliance or checklist adherence, but a nuanced socio-technical process shaped by trust, experience, collaboration, and adaptation. The diversity of approaches, the emergence of bespoke or hybrid "Franken-frameworks," and the influence of both internal and external factors underscore the need for flexible, context-sensitive strategies that can evolve alongside threats and technologies.

At the macro level, the diversity of CSRI&A approaches revealed in this study has implications beyond the boundaries of individual organizations. Patterns of framework hybridization, adaptation to regulatory mandates, and the spread of bespoke practices collectively shape the cybersecurity posture of national critical infrastructure sectors. As regulatory bodies and sector policymakers seek to set standards and encourage best practices, attention to ground-level decision-making and its inherent flexibility will be crucial. Policymakers should recognize that managerial discretion and organizational adaptation are not obstacles but vital components of systemic resilience, enabling critical infrastructure owners and operators to respond effectively to evolving cyber threats.

Looking forward, the findings invite both scholars and practitioners to embrace the complexity inherent in cybersecurity risk management. As new frameworks, measurement tools, and technologies—such as generative AI—continue to emerge, the field must remain open to innovation while being grounded in an empirical understanding of what works in practice. By

fostering ongoing dialogue between research and real-world application, and by prioritizing adaptability, transparency, and collaboration, organizations can strengthen their resilience and better safeguard critical infrastructure in an ever-changing digital environment.

Appendix A. Interview Questions

The following interview questions were approved under UMD IRB project 1628220-1.

Background fact-finding to be obtained on my own prior to the interview
Individual

- Current job title
- Current and total time working in cybersecurity & cybersecurity management
- Experience in the public, private, or mixed sectors
- Educational background: fields of study, degrees, certifications
- Professional associations
- Relevant service

Organizational

- Size of organization
- Type of organization (private, public, tier of government, quasi-governmental, etc.)
- Specific areas of work (type of critical infrastructure, place within the critical infrastructure network)
- Geographic location

Pilot study interview questions

Script: Thanks for taking the time to meet with me today and help me understand the cybersecurity risk space for my dissertation. I have about 20 question areas in three groups which should take us about 45 minutes to complete. If it's alright with you, let's begin.

First, I'd like to learn a little more about you.

(1) How would you describe your job to someone else?

Q2 should build on what was learned in the pre-interview fact-finding; use CV, LinkedIn, etc. to customize this question & follow-up to the respondent—probe beyond job titles.

(2) How did you come to do this type of work?

(3) Some sources consider the identification and assessment aspects of understanding risk as separate elements, others view them as a single element. How do you view identification and assessment of risk and why?
Use this answer to modify future reference of risk identification & assessment, matching response to questions below.
Alternate separate and single word order between interviews to see about order effects.

a. *If not already explicit*, can you tell me specifically about the risk identification and assessment parts of your job?

(4) What do you find most challenging, whether easy or hard, if anything, about conducting cybersecurity risk identification and assessments in your role as a [public or private or other type of] cybersecurity manager?

(5) How, if at all, did your understanding of risk identification and assessment change along this professional journey?

(6) Similarly, how, if at all, has the understanding of risk identification and assessment changed within your organization?

Script: Next, I'd like to ask about obtaining new cybersecurity risk identification and assessment information.

(7) Through what means do you learn about cybersecurity risk identification and assessment? Example could include but are not limited to conferences, invited talks, blogs, social media, articles, client visits, face-to-face meetings, phone, and email.
   a. Which of those means have you found to be the most effective? Why?
   Probes:
   b. How do you keep up with the latest in cybersecurity?
   c. How do you keep up with the latest in risk identification and assessment?
   d. How do you keep up with the latest in critical infrastructure?

(8) Have other colleagues, in or out of government, come to you suggesting that you use specific ways to identify and assess risk that you don't use already? If so, what sort of colleagues offered the suggestions and what did they suggest?
   a. What about product vendors? Did they make any suggestions, and if so what?
   b. Conversely, have you sought out colleagues, vendors, or both to learn about new approaches?
   c. What were these experiences like? How did they shape your decision to use those approaches or not? Did you adopt any of these suggestions, why yes or no?

Script: Great, let's shift gears a bit to discuss the work you do.

(9) Can you tell me about the time you last did a risk identification and assessment? Please describe what you did.
   a. *If they do not actually conduct the risk identification and assessment:*
   Can you walk me through your org chart to a person or team that does risk identification and assessment and tell me what they would do?
   Change pronouns / person orientation in Q10 and Q11 & Q12 as needed to reflect the 3rd person work.

Listen for cues regarding approaches mentioned, use in follow-ups & probes.

(10) How frequently do you conduct these? Are they regularly scheduled or externally triggered?

(11) Do you provide reports based on your risk identification and assessment work?
   a. For whom do you write these reports?
   If pushed back on whom, suggest e.g., tech people, upper mgmt., both, else.

b. How is your current risk identification and assessment process to generate useful reports?
   If pushed back on the how, suggest useful in terms of metrics in that report, e.g. financial loss, up/down time, IT/org/enterprise triangle, qualitative description.

(12) Are the risk identification and assessment processes you use documented somewhere?
   a. How frequently are these processes reviewed?
   b. *If reviewed*, what does this sort of evaluation look like? How do you assess if that process is meeting your needs and learn what to improve?

(13) What challenges do you encounter when completing your cybersecurity risk identification and assessment?
   a. *If any are named,* do you think they would affect the identification and assessment enough to give incorrect results?
   b. *If any are named,* How and why do you think that is?

(14) If no specific approaches are named in the last risk identification and assessment; proceed and ask the top question; if unsure or no response, offer suggestions; otherwise, skip to first follow-up.
   When you need did that last risk identification and assessment, what sort of risk methods, models, software, management practices, or other approaches did you use?
   Approach suggestions: NIST-RMF, OCTAVE, FAIR
   a. How did you learn about and being skilled at using the [named approach]?
   b. Why did you use the [named approach] for as part of that last risk identification and assessment?
   c. How useful do you feel is the [named approach]?
      Consider flipping b & c between interviews in case of question order effects.
   d. I'm going to list a few other reasons someone would use [named approach]. Please tell me which, if any, of them apply to you: *Omit any already stated*:
      Manager instruction, Team/Unit decision, Organization policy, External/Higher-level organization policy, Following a prescribed risk management standard.
   Ask a, b, c, & d again for each approach named.

(15) Are there any risk identification and assessment types of approaches you used to use but do not use any more?
   a. Why did you stop using it?
   b. If the reason was not up to the participant, would you still use it if you could?
   c. Are there any other approaches you no longer use that you would like to tell me about?
   d. Are there any approaches you intentionally decided not to use after learning about it?

(16) If any of the following are not already stated, Probe: Regarding other selection aspects:
   a. Did you inherit any risk identification and assessment approaches from your predecessor?
   b. *If applicable*, what sort of instruction, if any, do you receive upper management to use or consider using certain approaches for risk assessment?
   c. What role does the cost of a risk assessment tool play in its consideration for use?

d. What role does the impact of using [named approach] have on your systems factor into consideration for its use?
e. How much independence do you have to choose the approaches you want?

(17) Are there any programs, policies, procedures, and/or parts of the organization and its people that you or your organization does not yet have in place but you think would improve a cybersecurity risk identification and assessment?
   a. *If any are named,* what is it about them that would improve the identification and assessment?
   b. Why do you think that is?

(18) Are there any other policies, government wide or otherwise, that affect what risk identification and assessment approaches you can or cannot access?
   If affecting external policy was not yet discussed, probe here
   a. How do you see your role and capacity to affect external policy?

(19) As I go through this study, I may need additional information. Would you be willing to participate in:
   a. A follow-up interview,
   b. A survey,
   c. A focus group?

(20) Is there anything else you'd like to add with respect to what we've talked about today?

Appendix B. Survey Question Construction

Table 40

*Example Survey Question Development from the Literature**

Survey	Topic areas	Source	Source content (Exact wording in italics)	Usage in this study
Q1	Management level	Deloitte-NASCIO (2016, 2018)	Reports show C-Suite becoming more active in cybersecurity decisions (Not a question, statements from survey overview.)	Inspired to distinguish level of management
Q2	Amount of engagement with CSRI&A activities	Whitman & Mattard (2020: 45-57); (Deloitte & NASCIO, 2018: 244-254); see also Interviews	Whitman & Mattard (2020) discussed differences by leadership, but Deloitte & NASCIO (2018) had them also by sector (Not a specific question; has textbook discussion)	Inspired to directly ask frequency of activity to cross-reference with management level and sector
Q3	Who leads the approaches in the org. chart	Whitman & Mattard (2020: 230-241)	Chapter 5 shows variation within org. for primary responsibility for your organization's risk identification and assessment? (Not a specific question; Textbook style statements given and example org. chart structures.)	Inspired by Chapter 5 on developing the security program; also interview responses
Q4	Outsourcing approaches	Norris et al. (2021: 1180); see also (Deloitte & NASCIO, 2018) and Hatcher et al. (2020)	Does your local government outsource its cybersecurity responsibility?	Adapted local government to organization and added if risk identification and assessment were also outsourced

Survey	Topic areas	Source	Source content (Exact wording in italics)	Usage in this study
Q5	List of approaches used	Panagiotis et al. (2013: 41)	Please describe the risk assessment methodologies / models that you use or are considering to use?	Adapted question to approaches broadly and from considering to does note, does not anymore, and does use.
Q6	Are approaches used sufficient	n/a	n/a	No longer use Use but not sufficient Use and is sufficient
Q7	Approaches for IT, OT, & CPS	Parsons (2018)	Identified distinctions of OT and IT operations (Not a specific question)	Inspired IT/OT use question
Q8	Bespoke approach	n/a	n/a	Please describe process
Q9	IT/OT approach challenges	n/a	n/a	Select any/all reasons why approaches are challenging for your CSRI&A needs
Q10	Describing approach selection process	Panagiotis et al. (2013: 43)	Please describe the process used or considered for validating your risk analysis approaches	Adapted validating to selecting and risk analysis to risk identification and assessment
Q11	Deeper Dive into 1 approach	See Appendix D.	See Appendix D.	See Appendix D.
Q12	Type of org.	Norris et al. (2021); see also (Deloitte & NASCIO, 2018)	Entire paper is about local government, compared to most at national level (Not a specific question)	Inspired asking about type of org.; differences between government & industry

Survey	Topic areas	Source	Source content (Exact wording in italics)	Usage in this study
Q13	Critical infrastructure sectors	(Deloitte & NASCIO, 2018: 9)	Tables & discussion show differences by operational sectors (Sourced from results table, not a question)	Adapted from federal cabinet agency sectors to CISA sectors
Q14	Org. size	Whitman & Mattard (2020: 225-230)	Which best describes the personnel size your organization? (Not a specific question, but discussed needs and strategies in small, medium, and large orgs.)	Inspired question; relation between org size, its resources, and allocation for security; Chapter 5—adapted focus from computers to people
Q15	Year of experience	Norris et al. (2021: 1178)	Asked for IT experience in year ranges (from result table)	Adapted for cybersecurity
Q16	Association membership	Whitman & Mattard (2020: 24-264)	Org. oversight of the professional certifications (Not a specific question; detailed cert. awarding orgs and their role in training cyber management.)	Inspired to ask open answer
Q17	Certifications as a measure of education and expertise	Whitman & Mattard (2020: 244-264)	Which, if any, cybersecurity or risk management related certifications do you hold? (Not a specific question; has textbook review of cert types and purposes for staffing strategies)	Inspired Chapter 5 and values of topic-specific certifications; also interview responses
Q18	Level of education	n/a	n/a	Boilerplate
Q19	Race / Ethnicity	n/a	n/a	Boilerplate

Survey	Topic areas	Source	Source content (Exact wording in italics)	Usage in this study
Q20	Gender identity	n/a	n/a	Boilerplate
Q21	Anything else to add	n/a	n/a	Boilerplate

B.1 Surveys in Qualtrics

- These questions were approved under UMD IRB project 1628220-2.
- There will be an allowance to add a one additional question to organizations that help share this survey with their members / audience.
- Participants must complete an initial survey to log their consent and option to receive an executive summary. The link in the thank you of the initial survey then launches the regular survey.
- Question are screenshots from Qualtrics, and question numbers are for review reference only; they do not appear in Qualtrics.
- The survey consent form is very similar to the interview consent form
- The back button on surveys is intentionally disabled.
- You can view & test either of the surveys:
    - Consent form survey: https://umdsurvey.umd.edu/jfe/form/SV_2beCk0QmH7UnqJM
    - Regular survey: https://umdsurvey.umd.edu/jfe/form/SV_0Os6yjymMmDKR8y

B.2 Consent Survey in Qualtrics

UNIVERSITY OF MARYLAND

This survey is designed to help learn what cybersecurity risk identification and assessment approaches you use, why you use them, and things you consider important when selecting them. Your responses will help to develop research and practice that focuses on user and organizational cybersecurity risk preferences, as well as help inform new approach development.

Definition: This survey defines “approaches” as any of the diverse options to help understand risk identification and assessment which include but are not limited to methods, models, frameworks, guidance, procedures, software, and other tools.

This survey will not ask questions sensitive to your cybersecurity risk operations. If you interpret a question as being sensitive, please feel free to abstract your response or skip the question.

This survey consists of:
1 participation consent form,
4 introductory questions about you and your organization,
3-5 questions about what approaches you use,
1 large question block about approach importance,
3 quick organization background questions,

6 quick individual demographic questions,
1 final question about for anything else you want to share.

Informed Consent to Participate in a Research Study

Study Title

Selecting Cybersecurity Risk Identification and Assessment Approaches for Critical Infrastructure

You are being invited to participate in a research study. This consent form will provide you with information on the research project, what you will need to do, and the associated risks and benefits of the research. Your participation is voluntary. Please read this form carefully. It is important that you fully understand the research and are able to ask questions in order to make an informed decision. You have the option to print and/or download a copy of this consent form to keep.

Purpose

This research is being conducted by me, Principal Investigator Shawn Janzen, at the University of Maryland, College Park as part of my dissertation. I am inviting you to participate in this research project because of your professional expertise in the areas of critical infrastructure and cybersecurity. The purpose of this research project is to better understand the selection of approaches used to support cybersecurity risk identification and assessment.

Procedures

The Principal Investigator will collect data about decision making, processes, management, and policy that may guide the cybersecurity risk identification and assessment of critical infrastructure. That data will come from through interviews, a survey, and policy document analysis. This portion of the data collection pertains to the survey which will ask about cybersecurity risk approaches and your preferences, usage, and views of those approaches. The estimated times to complete this survey is 30 minutes.

Benefits

As a direct benefit for participating in this research, I will provide you with an option to receive an executive summary of larger trends in the study results. This summary will be emailed to the address you provide and will be provided once the dissertation connected with this project is complete. More broadly, your participation in this study will help better understand theory and practice of cybersecurity risk management and policy.

Risks and Discomforts

There are no anticipated risks beyond those encountered in everyday life.

Privacy and Confidentiality

No identifying information will be collected. Your signed consent form and optionally provided email address for the executive summary will both be kept separate from your survey data, and responses will not be linked to you.

Your survey-related information will be kept confidential within the limits of the law. Any

identifying information will be kept in a secure location and only the project researchers will have access to the data. Survey participants will not be identified in any publication or presentation of research results; only aggregate data will be used.

Voluntary Participation
Taking part in this research survey is entirely up to you. You may choose not to participate or you may discontinue your participation at any time without penalty or loss of benefits to which you are otherwise entitled.

Contact Information
If you have any questions or concerns about this research, you may contact Principal Investigator Shawn Janzen at 847-514-6677. This project has been approved by the University of Maryland Institutional Review Board. If you have any questions about your rights as a research participant or complaints about the research, you may call the Institutional Review Board (IRB) at 301-405-0678 or email irb@umd.edu. IRB Reference Number 1628220-1.

Optional: Click here if you would like to download a pdf copy of the consent form.
This will open a new browser tab from which you can save the consent form to your computer, or right-click and choose 'Save As' to directly download the pdf file.

Consent Statement and Signature
I have read this consent form and have had the opportunity to have my questions answered to my satisfaction. I voluntarily agree to participate in this study and am over the age of 18. I understand that, before I begin participation, a downloadable copy of this consent form is available to me.

Please enter your first and last name in the box below.
By typing your name below, you consent to participating in this research study.
If you have questions before consenting, please contact us using the contact information above.
If you do not consent, please do not enter your name and exit this survey.
You may exit this survey at any time by closing the browser window / tab.

Optional Executive Summary
Your participation in my study is greatly appreciated. As a thank you, I can send you an executive summary of this research when the study is complete. If you would like a copy, please enter your email address below.

→

Thank you. Your consent and optional email address were recorded.

Please click the link below to begin the survey questions:
https://umdsurvey.umd.edu/jfe/form/SV_0Os6yjymMmDKR8y

B.3 Regular Survey in Qualtrics

(UMD logo omitted to preserve image breaks across pages)

Q1

What level of management best describes your position?

- ○ Front-line operational manager
- ○ Mid-level manager
- ○ Senior manager or Director
- ○ Chief Officer

Q2

How frequently do you engage in risk identification and assessment activities as part of your cybersecurity management position?

- ○ Not at all
- ○ Rarely
- ○ Sometimes
- ○ Frequently
- ○ Regularly

Q3

Which group(s) in your organization have primary responsibility for your organization's risk identification and assessment? (Check more than one option if the primary responsibility is shared and/or if those groups are part of the same unit in your org chart.)

- ☐ IT team
- ☐ Security team
- ☐ Finance team
- ☐ Insurance team
- ☐ Internal audit team
- ☐ Separate risk management team
- ☐ It is outsourced
- ☐ Other:

.

Q4

Does your organization outsource any of the following functions? (Check all that apply)

- [ ] Cybersecurity
- [ ] Risk identification and assessment

→

Q5

Think about the cybersecurity risk identification and assessment at your organization.

Which of the following approaches, if any, do you currently use or have used before as part of your cybersecurity risk identification and assessment processes at your organization? (Change button to Yes)

	No	Yes
NIST Risk Management Framework (RMF)	●	○
NIST Cybersecurity Framework (CSF)	●	○
NIST Special Publication 800-53	●	○
NIST Special Publication 800-171	●	○
ISO 27001	●	○
ISO 27005	●	○
ISO 31000	●	○
Factor Analysis of Information Risk (FAIR)	●	○
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	●	○
MITRE Shield / MITRE Engage	●	○
MITRE ATT&CK	●	○
CIS 20 or Critical Security Controls (CSC)	●	○
Control Objectives for Information Related Technology (COBIT)	●	○
Capability Maturity Model Integration (CMMI)	●	○
Cybersecurity Maturity Model Certification (CMMC)	●	○
Tapestry	●	○
Custom in-house solution	●	○
Other #1	●	○
Other #2	●	○
Other #3	●	○

→

Q6

(Using examples selected from Q5 to demonstrate carry forward feature.)

In the question below, I ask you about approaches you said you use.

If you entered an "Other" approach option, this survey system was unable to display the name, so I am listing it here for you as a reminder. You do not need to enter the "Other" name again below.

Other #1: Screenshot Example

Which of the following best applies to the cybersecurity risk identification and assessment approaches you use?

	No longer use	Use but it is NOT sufficient	Use and it IS sufficient
NIST Special Publication 800-53	○	○	○
Tapestry	○	○	○
Custom in-house solution	○	○	○
Other #1	○	○	○

→

Q7

Do you use the previously mentioned approaches for: (Check all that apply)

- ☐ Information technologies (IT)
- ☐ Operational technologies (OT)
- ☐ Cyber physical systems (CPS; convergence of IT + OT)

→

Q8
(Shown only if selecting custom response from Q5.)

You mentioned using a custom in-house cybersecurity risk identification and assessment approach. Please briefly tell me about it.
For example, was it developed entirely in-house or were others, such as consultants, involved? Was it a prompted by upper management or front-line staff? Which, if any, other approaches inspired this custom approach?

Q9
(Shown only if selecting OT or CPS response from Q7.)

Since you mentioned OT / CPS, do you find any of the following reasons challenging to select a cybersecurity risk identification and assessment approach for your OT / CPS needs? (Check all that apply)

- [ ] Approaches tend to be too IT focused
- [ ] Lack of good approaches for OT and/or CPS
- [ ] Other

Q10

Please describe the process you use or consider for selecting your risk identification and assessment approaches for critical infrastructure cybersecurity.

→

Q11.0

(Questions are sub-numbered here to help reference groups of responses. All of question 11 appears on the same page. All response options within a group will appear in random order.)

In the question below, I want to take a deeper look at just one approach you use.
There are many responses for this question, but this you're almost done after this.

Choose one of the approach from the drop menu below. Think about the approach you select for the next set responses.

If you provided "Other" approaches, unfortunately this survey system was unable to display those names in the drop menu, so I am listing them here for you as a reminder.

Other #1: Screenshot Example

For the questions below, please rate the importance of each following statements for why you currently use that approach for your organization's cybersecurity risk identification and assessment, where 1: strongly disagree; 2: moderately disagree, 3: somewhat disagree, 4: neutral (neither disagree nor agree), 5: somewhat agree, 6: moderately agree, and 7: strongly agree.

Q11.1

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
The results of using the approach are apparent to me.	○	○	○	○	○	○	○
Suggested or instructed by upper management or an advisory group to use this approach.	○	○	○	○	○	○	○
I will recommend others within my organization to use this approach.	○	○	○	○	○	○	○
Using approach helps me to accomplish things more quickly.	○	○	○	○	○	○	○
This approach has a low impact on organizational systems and operations.	○	○	○	○	○	○	○
I saw this approach demonstrated at an event (seminar, workshop, conference, etc.).	○	○	○	○	○	○	○

Q11.2

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
Given the resources, opportunities and knowledge it takes to use this approach, it would be easy for me to customize this approach for my or my organization's needs.	○	○	○	○	○	○	○
People whose opinions that I value prefer that I use this approach.	○	○	○	○	○	○	○
Use of this approach was carried over from previous person in my position	○	○	○	○	○	○	○
I find the approach to be useful in my job.	○	○	○	○	○	○	○
I intend to continue using this approach in the future.	○	○	○	○	○	○	○
This approach is a good value for the money.	○	○	○	○	○	○	○

Q11.3

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
I am successful using this approach because I used similar approaches before this one for the same needs.	○	○	○	○	○	○	○
Colleagues outside my organization recommended using this approach.	○	○	○	○	○	○	○
I saw / heard this approach was used by another organization that interests me.	○	○	○	○	○	○	○
Using the approach enhances my effectiveness in my job.	○	○	○	○	○	○	○
This approach is useful for communicating / reporting with my peer / subordinate managers and front-line staff.	○	○	○	○	○	○	○
I have control over using this approach.	○	○	○	○	○	○	○

Q11.4

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
I like working through certain parts of using this approach.	○	○	○	○	○	○	○
My interaction with the approach is clear and understandable.	○	○	○	○	○	○	○
Using the approach in my job increases my productivity.	○	○	○	○	○	○	○
Although it might be helpful, using the approach is certainly not compulsory in my job.	○	○	○	○	○	○	○
I use this approach because of regulatory compliance requirements.	○	○	○	○	○	○	○
I use this approach because of internal policy compliance requirements.	○	○	○	○	○	○	○

Q11.5

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
My organization's vendor or consultant recommended using this approach.	○	○	○	○	○	○	○
This approach is useful for communicating / reporting with my upper management or advisory group.	○	○	○	○	○	○	○
I am successful using this approach because I had the independence to use it how I wanted.	○	○	○	○	○	○	○
I am successful using this approach because I had the product support team.	○	○	○	○	○	○	○
In my job, usage of this approach is important.	○	○	○	○	○	○	○
I use this approach because of policies from outside my organization not related to regulatory or insurance compliance requirements.	○	○	○	○	○	○	○

Q11.6

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
If I use other approaches, I plan to use this approach along with the other approaches.	○	○	○	○	○	○	○
My supervisor does not require me to use the approach.	○	○	○	○	○	○	○
I have the knowledge necessary to use this approach.	○	○	○	○	○	○	○
I find the approach to be easy to use.	○	○	○	○	○	○	○
I have no problem with the quality of this approach's output.	○	○	○	○	○	○	○
People who influence my behavior think that I should use this approach.	○	○	○	○	○	○	○

Q11.7

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
I believe I could communicate to others the consequences of not using the approach.	○	○	○	○	○	○	○
This approach is cost efficient on organizational finances and personnel.	○	○	○	○	○	○	○
This approach has quantitative / numeric measures useful for analysis and reporting	○	○	○	○	○	○	○
In my job, usage of this approach is relevant.	○	○	○	○	○	○	○
It is easy for me to become skillful at using approach.	○	○	○	○	○	○	○
I am successful using this approach because I had support documentation materials.	○	○	○	○	○	○	○

Q11.8

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
This approach is compatible with other approaches I use.	○	○	○	○	○	○	○
I am successful using this approach because someone showed me how to do it first.	○	○	○	○	○	○	○
I find using the approach to be enjoyable.	○	○	○	○	○	○	○
The quality of the output I get from the approach is high.	○	○	○	○	○	○	○
This approach is reasonably priced.	○	○	○	○	○	○	○
In general, my organization has supported the use of this approach.	○	○	○	○	○	○	○

Q11.9

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
The actual process of using this approach is pleasant.	○	○	○	○	○	○	○
This approach has qualitative / descriptive measures useful for analysis and reporting	○	○	○	○	○	○	○
The use of the approach is pertinent to my various job-related tasks.	○	○	○	○	○	○	○
Risk management or cybersecurity operations experts I value recommended using this approach.	○	○	○	○	○	○	○
I rate the results from this approach to be excellent.	○	○	○	○	○	○	○
I have no difficulty telling others about the results of using the approach.	○	○	○	○	○	○	○

Q11.10

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
My use of the approach is voluntary.	○	○	○	○	○	○	○
I have the resources necessary to use this approach.	○	○	○	○	○	○	○
This approach broadly accounts for threats, vulnerabilities, and consequences	○	○	○	○	○	○	○
This approach was listed as a best practice	○	○	○	○	○	○	○
I will recommend others outside my organization to use this approach.	○	○	○	○	○	○	○
I use this approach because of cyber insurance compliance requirements.	○	○	○	○	○	○	○
I find the approach to be easy to use.	○	○	○	○	○	○	○

→

Q12

Which sector best describes your organization type

- ○ Federal government
- ○ State government
- ○ Local or Tribal government
- ○ Quasi-government
- ○ Private, for-profit organization
- ○ Private non-profit organization
- ○ Public, for-profit organization
- ○ Public, non-profit organization
- ○ Other:

Q13

Which of the following critical infrastructure sectors best applies to your organization's area of work? (Check all that apply)

- [ ] Chemical
- [ ] Commercial facilities
- [ ] Communications
- [ ] Critical manufacturing
- [ ] Dams
- [ ] Defense industrial base
- [ ] Emergency services
- [ ] Energy
- [ ] Financial services
- [ ] Food and agriculture
- [ ] Government facilities
- [ ] Health and public health
- [ ] Information technology
- [ ] Nuclear reactors, materials, and waste
- [ ] Transportation systems
- [ ] Water and wastewater systems

Q14

Which best describes your organization's personnel size?

- ○ Less than 10 people
- ○ 10 - 100 people
- ○ 101 - 1,000 people
- ○ 1,001 - 10,000 people
- ○ 10,001 - 25,000 people
- ○ More than 25,000 people

→

Q15

How many years total have you worked in cybersecurity management?

- 0-5 years
- 6-10 years
- 11-20 years
- 21+ years

Q16

With which, if any, professional associations do you identify as a member?

Examples: (ISC)^2, ISACA, AFFIRM, RIMS.

Q17

Which, if any, cybersecurity or risk management related certifications do you hold?

Examples: CISSP, CWNA, SSCP, CRM, PMP

Q18

What is your highest level of education?

- Less than high school
- High school diploma or equivalent
- Associate's degree
- Bachelor's degree
- Master's degree
- Doctoral degree
- Other terminal graduate degree, e.g., Juris doctor

Q19

What is your race and/or ethnic origin(s)?

Q20

What is your gender identity?

→

Q21

Is there anything else you would like to share with me regarding the selection of risk identification and assessment approaches for critical infrastructure cybersecurity?

Thank you! Click the arrow below to submit your responses.

→

Your responses have been recorded.

Thank you for your time and effort spent taking this survey.
Your participation is greatly appreciated.

If you have any questions about this survey or any other aspect of the research study that will use this survey,
please email me: Shawn Janzen at sjanzen@umd.edu.

Appendix C. Mapping the Interview to the Research Questions

The following **Error! Reference source not found.** maps the conceptual framework to the interview questions and the interview questions to the research questions. The first column indicates an assumed estimate as to how frequently that construct will code to that interview question.

Table 41

Mapping the Conceptual Framework to Interview and Research Questions

Conceptual Framework Construct (Estimated relationship)	Interview Question	Research Question
Foundational: high Functional: low Situational: low	Q1) Job description	RQ1 (what), RQ2 (why)
Foundational: high Functional: low Situational: low	Q2) Professional experience	RQ1 (what), RQ2 (why)
Foundational: high Functional: high Situational: none	Q3) Understanding risk I&A stages	RQ2 (why)
Foundational: low Functional: high Situational: high	Q4) Challenges conducting risk I&A	RQ1 (what), RQ2 (why)
Foundational: high Functional: high Situational: high	Q5) How did risk I&A change over time (self)	RQ2 (why),
Foundational: high Functional: high Situational: high	Q6) How did risk I&A change over time (organization)	RQ2 (why),
Foundational: high Functional: high Situational: high	Q7) Learning about risk I&A, cybersecurity, and critical infrastructure	RQ1 (what), RQ2 (why)
Foundational: none Functional: high Situational: high	Q8) Suggested approaches	RQ1 (what), RQ2 (why)

Foundational: low Functional: high Situational: high	Q9) Last time you did a risk I&A	RQ2 (why)
Foundational: low Functional: high Situational: high	Q10) Risk I&A frequency and scheduling	RQ2 (why)
Foundational: low Functional: high Situational: high	Q11) Risk I&A reporting	RQ2 (why)
Foundational: low Functional: high Situational: high	Q12) Risk I&A documentation	RQ2 (why)
Foundational: high Functional: high Situational: high	Q13) Challenges conducting risk I&A	RQ2 (why)
Foundational: low Functional: high Situational: high	Q14) What approaches used	RQ2 (why)
Foundational: low Functional: high Situational: high	Q15) What approaches no longer used	RQ2 (why)
Foundational: low Functional: high Situational: high	Q16) Possible approach influence from: predecessor, upper management, cost, system impact, independence	RQ2 (why)
Foundational: high Functional: high Situational: high	Q17) Programs, policies, procedures, or parts of the organization not in place	RQ1 (what), RQ2 (why)
Foundational: high Functional: Situational: high	Q18) Other policies that may affect selection	RQ1 (what), RQ2 (why)
n/a	Q19) Follow up contact	n/a
Possibly any	Q20) Anything else to add	Possibly any

Appendix D: Mapping Survey Battery Question from the Literature and Preliminary Interview Data

Shawn's adapted construction of the survey battery question, built from previous acceptance models and Shawn's interview data.

Modifications to previous survey items include changing 2 terms:
1) computer → cybersecurity risk identification and assessment
2) system → approach
My survey battery uses a 7-point Likert scale, in line with most of the TAM3 and UTAUT2 models' items.

> "Using the approach you selected from the droplist above, please rate the importance of each following statements for why you currently use that approach for your organization's cybersecurity risk identification and assessment, where 1: strongly disagree; 2: moderately disagree, 3: somewhat disagree, 4: neutral (neither disagree nor agree), 5: somewhat agree, 6: moderately agree, and 7: strongly agree." (Shawn's survey)

In the table below, constructs marked in dark grey were not used. Items marked green are my new contributing additions.

Table 42

Mapping Survey Battery Questions from the Literature and Preliminary Interview Data

UTAUT2 Construct	**UTAUT2 Item Code**	**UTAUT2**	**Modified UTAUT2**	**TAM3 Item**	**TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)**	**From Interview (Early Qualtrics Survey)**	**My Survey Item**	**My Framework Construct Alignment**
		Venkatesh et al. (2012)	Ford, 2021					
Performance Expectancy (PE)	PE1	I find mobile Internet useful in my daily life	I would find artificially intelligent security tools useful in my daily life.	PU4	I find the system to be useful in my job.		I find the approach to be useful in my job.	Functional &/or Situational

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
	PE2	Using mobile Internet increases my chances of achieving things that are important to me. (dropped)						
	PE3	Using mobile Internet helps me accomplish things more quickly.	Using artificially intelligent security tools helps me to accomplish things more quickly.				Using approach helps me to accomplish things more quickly.	Functional
	PE4	Using mobile Internet increases my productivity.	Using artificially intelligent security tools increases my productivity	PU2	Using the system in my job increases my productivity.		Using the approach in my job increases my productivity.	Functional
	PE5		If I use artificially intelligent security tools, I will increase my chances of getting a raise.			Listed as a best practice	This approach was listed as a best practice	Functional &/or Situational
				PU1	Using the system improves my performance in my job			

UTAUT2 Construct	**UTAUT2 Item Code**	**UTAUT2**	**Modified UTAUT2**	**TAM3 Item**	**TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)**	**From Interview (Early Qualtrics Survey)**	**My Survey Item**	**My Framework Construct Alignment**
				PU3	Using the system enhances my effectiveness in my job.		Using the approach enhances my effectiveness in my job.	Functional
Effort Expectancy (EE)	EE1	Learning how to use mobile Internet is easy for me.	Learning how to use artificially intelligent security tools is easy for me.	PEOU3	I find the system to be easy to use.		I find the approach to be easy to use.	Functional
	EE2	My interaction with mobile Internet is clear and understandable.	My interaction with artificially intelligent security tools is clear and understandable.	PEOU1	My interaction with the system is clear and understandable.		My interaction with the approach is clear and understandable.	Foundational
	EE3	I find mobile Internet easy to use.	I find artificially intelligent security tools easy to use.	PEOU3	I find the system to be easy to use.		I find the approach to be easy to use.	Functional
	EE4	It is easy for me to become skillful at using mobile Internet.	It is easy for me to become skillful at using artificially intelligent security tools.				It is easy for me to become skillful at using approach.	Functional &/or Foundational
				PEOU4	I find it easy to get the system to do what I want it to do.			

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
Social Influence (SI)	SI1	People who are important to me think that I should use mobile Internet.	People who are important to me think that I should use artificially intelligent security tools.	SN2	People who are important to me think that I should use the system.			
	SI2	People who influence my behavior think that I should use mobile Internet.	People who influence my behavior think that I should use artificially intelligent security tools.	SN1	People who influence my behavior think that I should use the system.		People who influence my behavior think that I should use this approach.	Situational
	SI3	People whose opinions that I value prefer that I use mobile Internet.	People whose opinions that I value prefer that I use artificially intelligent security tools.				People whose opinions that I value prefer that I use this approach.	Situational
	SI4		In general, my organization has supported the use of artificially intelligent security tools.	SN4	In general, the organization has supported the use of the system.		In general, my organization has supported the use of this approach.	Functional &/or Situational
				SN3	The senior management of this business has been helpful in the use of the system.			

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
						Recommended by colleague outside my organization	Colleagues outside my organization recommended using this approach.	Functional &/or Situational
						Recommended by my organization's vendor or consultant	My organization's vendor or consultant recommended using this approach.	Functional &/or Situational
						Saw it demonstrated at an event (seminar, workshop, conference, etc.)	I saw this approach demonstrated at an event (seminar, workshop, conference, etc.).	Functional &/or Situational
						Saw / Heard it was used by another organization that interests me	I saw / heard this approach was used by another organization that interests me.	Functional &/or Situational
						Recommended by risk management or cybersecurity operations experts in my organization	Risk management or cybersecurity operations experts I value recommended using this approach.	Any of the 3

UTAUT2 Construct	**UTAUT2 Item Code**	**UTAUT2**	**Modified UTAUT2**	**TAM3 Item**	**TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)**	**From Interview (Early Qualtrics Survey)**	**My Survey Item**	**My Framework Construct Alignment**
Facilitating Conditions (FC)	FC1	I have the resources necessary to use mobile Internet.	I have the resources necessary to use artificially intelligent security tools.	PEC2	I have the resources necessary to use the system.		I have the resources necessary to use this approach.	Functional &/or Situational
	FC2	I have the knowledge necessary to use mobile Internet.	I have the knowledge necessary to use artificially intelligent security tools.				I have the knowledge necessary to use this approach.	Foundational
	FC3	Mobile Internet is compatible with other technologies I use.	Artificially intelligent security tools are compatible with other technologies I use.				This approach is compatible with other approaches I use.	Functional &/or Situational
				PEC1	I have control over using the system.		I have control over using this approach.	Situational
				PEC4	The system is not compatible with other systemes I use.			
				PEC3	Given the resources, opportunities and knowledge it takes to use the system, it would be easy for me to use the system.		Given the resources, opportunities and knowledge it takes to use this approach, it would be easy for me to customize this approach for my or my organization's needs.	Any of the 3

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
	FC4	I can get help from others when I have difficulties using mobile Internet.	I have the necessary assistance when I have difficulties using artificially intelligent security tools.			Internal policy compliance requirement	I use this approach because of internal policy compliance requirements.	Situational
						Cyber insurance compliance requirement	I use this approach because of cyber insurance compliance requirements.	Situational
						Regulatory compliance requirement	I use this approach because of regulatory compliance requirements.	Situational
						Other external policy / compliance requirement (not regulatory or insurance)	I use this approach because of policies from outside my organization not related to regulatory or insurance compliance requirements.	Situational
Hedonic Motivation (HM)	HM1	Using mobile Internet is fun.	Using artificially intelligent security tools is fun.	ENJ3	I have fun using the system.		I like working through certain parts of using this approach.	Any of the 3
	HM2	Using mobile Internet is enjoyable.	Using artificially intelligent security tools is enjoyable.	ENJ1	I find using the system to be enjoyable.		I find using the approach to be enjoyable.	Any of the 3

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
	HM3	Using mobile Internet is very entertaining.	Using artificially intelligent security tools is very entertaining.	ENJ2	The actual process of using the system is pleasant.		The actual process of using this approach is pleasant.	Any of the 3
Price Value (PV)	PV1	Mobile Internet is reasonably priced.	Artificially intelligent security tools are reasonably priced.				This approach is reasonably priced.	Funcational
	PV2	Mobile Internet is a good value for the money.	Artificially intelligent security tools are a good value for the money.				This approach is a good value for the money.	Functional
	PV3	At the current price, mobile Internet provides a good value.	At the current price, artificially intelligent security tools provide a good value.					
						Cost efficient (financial and personnel)	This approach is cost efficient on organizational finances and personnel.	Functional
						Low impact on systems and operations	This approach has a low impact on organizational systems and operations.	Functional
Habit	HT1	The use of mobile Internet has become a habit for me.	The use of artificially intelligent security tools has become a habit for me.					

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
	HT2	I am addicted to using mobile Internet.	I am addicted to using artificially intelligent security tools.					
	HT3	I must use mobile Internet.	I must use artificially intelligent security tools.					
	HT4	Using mobile Internet has become natural to me. (dropped)						
Behavioral Intention (BI)	BI1	I intend to continue using mobile Internet in the future.	I intend to continue using artificially intelligent security tools in the future.	BI1	Assuming I had access to the system, I intend to use it.		I intend to continue using this approach in the future.	Any of the 3
	BI2	I will always try to use mobile Internet in my daily life.	I will always try to use artificially intelligent security tools in my daily life.					
	BI3	I plan to continue to use mobile Internet frequently.	I plan to continue to use artificially intelligent security tools frequently.					
				BI2	Given that I had access to the system, I predict that I would use it.			

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
				BI3	I plan to use the system in the next <n> months.			
							If I use other approaches, I plan to use this approach along with the other approaches.	Any of the 3
							I will recommend others outside my organization to use this approach.	Any of the 3
							I will recommend others within my organization to use this approach.	Any of the 3
Use Behavior (USE)	USE1	(Asked about frequency using different online technologies)	My personal use of artificially intelligent security tools.					
	USE2	(Asked about frequency using different online technologies)	My recommendation to use artificially intelligent security tools within my organization.					

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
	USE3	(Asked about frequency using different online technologies)	My recommendation to use artificially intelligent security tools outside of my organization.					
				VOL1	My use of the system is voluntary.		My use of the approach is voluntary.	Situational
				VOL2	My supervisor does not require me to use the system.		My supervisor does not require me to use the approach.	Situational
				VOL3	Although it might be helpful, using the system is certainly not compulsory in my job.		Although it might be helpful, using the approach is certainly not compulsory in my job.	Situational
						Suggested or instructed by upper management or advisory group	Suggested or instructed by upper management or an advisory group to use this approach.	Functional &/or Situational
						Carried over from previous person in my position	Use of this approach was carried over from previous person in my position	Situational

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
				REL1	In my job, usage of the system is important.		In my job, usage of this approach is important.	Any of the 3
				REL2	In my job, usage of the system is relevant.		In my job, usage of this approach is relevant.	Any of the 3
				REL3	The use of the system is pertinent to my various job-related tasks.		The use of the approach is pertinent to my various job-related tasks.	Any of the 3
				OUT1	The quality of the output I get from the system is high.		The quality of the output I get from the approach is high.	Functional
				OUT2	I have no problem with the quality of the system's output.		I have no problem with the quality of this approach's output.	Functional
				OUT3	I rate the results from the system to be excellent.		I rate the results from this approach to be excellent.	Functional

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
						Is useful for communicating / reporting with my upper management or advisory group	This approach is useful for communicating / reporting with my upper management or advisory group.	Any of the 3
						Is useful for communicating / reporting with my peer / subordinate managers and front-line staff	This approach is useful for communicating / reporting with my peer / subordinate managers and front-line staff.	Any of the 3
				RES1	I have no difficulty telling others about the results of using the system.		I have no difficulty telling others about the results of using the approach.	Any of the 3
				RES2	I believe I could communicate to others the consequences of using the system.		I believe I could communicate to others the consequences of not using the approach.	Any of the 3
				RES3	The results of using the system are apparent to me.		The results of using the approach are apparent to me.	Any of the 3

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
				RES4	I would have difficulty explaining why using the system may or may not be beneficial.			
						Broadly accounts for threats, vulnerabilities, and consequences	This approach broadly accounts for threats, vulnerabilities, and consequences	Any of the 3
						Has qualitative / descriptive measures useful for analysis and reporting	This approach has qualitative / descriptive measures useful for analysis and reporting	Functional
						Has quantitative / numeric measures useful for analysis and reporting	This approach has quantitative / numeric measures useful for analysis and reporting	Functional

UTAUT2 Construct	UTAUT2 Item Code	UTAUT2	Modified UTAUT2	TAM3 Item	TAM3 (Not used: Computer Playfulness, Computer Anxiety, Objective Usability, or Image)	From Interview (Early Qualtrics Survey)	My Survey Item	My Framework Construct Alignment
					I could complete the job using a software package . . .			
				CSE1	. . . if there was no one around to tell me what to do as I go.		I am successful using this approach because I had the independence to use it how I wanted.	Functional &/or Situational
				CSE2	. . . if I had just the built-in help facility for assistance.		I am successful using this approach because I had the product support team.	Situational
				CSE3	. . . if someone showed me how to do it first.		I am successful using this approach because someone showed me how to do it first.	Foundational
				CSE4	. . . if I had used similar packages before this one to do the same job.		I am successful using this approach because I used similar approaches before this one for the same needs.	Foundational &/or Situational
							I am successful using this approach because I had support documentation materials.	Situational

Appendix E. IRB Approvals

UNIVERSITY OF MARYLAND
INSTITUTIONAL REVIEW BOARD

1204 Marie Mount Hall
College Park, MD 20742-5125
TEL 301.405.4212
FAX 301.314.1475
irb@umd.edu
www.umresearch.umd.edu/IRB

DATE:	December 10, 2020
TO:	Shawn Janzen
FROM:	University of Maryland College Park (UMCP) IRB
PROJECT TITLE:	[1628220-1] Choosing cybersecurity risk identification and assessment approaches for critical infrastructure: A background exploration and pilot study proposal
REFERENCE #:	
SUBMISSION TYPE:	New Project
ACTION:	APPROVED
APPROVAL DATE:	December 10, 2020
EXPIRATION DATE:	December 9, 2021
REVIEW TYPE:	Expedited Review
REVIEW CATEGORY:	Expedited review category # 7

Thank you for your submission of New Project materials for this project. The University of Maryland College Park (UMCP) IRB has APPROVED your submission. This approval is based on an appropriate risk/benefit ratio and a project design wherein the risks have been minimized. All research must be conducted in accordance with this approved submission.

Prior to submission to the IRB Office, this project received scientific review from the departmental IRB Liaison.

This submission has received Expedited Review based on the applicable federal regulations.

This project has been determined to be a MINIMAL RISK project. Based on the risks, this project requires continuing review by this committee on an annual basis. Please use the appropriate forms for this procedure. Your documentation for continuing review must be received with sufficient time for review and continued approval before the expiration date of December 9, 2021.

Please remember that informed consent is a process beginning with a description of the project and insurance of participant understanding followed by a signed consent form. Informed consent must continue throughout the project via a dialogue between the researcher and research participant. Unless a consent waiver or alteration has been approved, Federal regulations require that each participant receives a copy of the consent document.

Please note that any revision to previously approved materials must be approved by this committee prior to initiation. Please use the appropriate revision forms for this procedure.

All UNANTICIPATED PROBLEMS involving risks to subjects or others (UPIRSOs) and SERIOUS and UNEXPECTED adverse events must be reported promptly to this office. Please use the appropriate reporting forms for this procedure. All FDA and sponsor reporting requirements should also be followed.

All NON-COMPLIANCE issues or COMPLAINTS regarding this project must be reported promptly to this office.

Please note that all research records must be retained for a minimum of seven years after the completion of the project.

If you have any questions, please contact the IRB Office at 301-405-4212 or irb@umd.edu. Please include your project title and reference number in all correspondence with this committee.

This letter has been electronically signed in accordance with all applicable regulations, and a copy is retained within University of Maryland College Park (UMCP) IRB's records.

UNIVERSITY OF MARYLAND
INSTITUTIONAL REVIEW BOARD

1204 Marie Mount Hall
College Park, MD 20742-5125
TEL 301.405.4212
FAX 301.314.1475
irb@umd.edu
www.umresearch.umd.edu/IRB

DATE:	February 24, 2021
TO:	Shawn Janzen
FROM:	University of Maryland College Park (UMCP) IRB
PROJECT TITLE:	[1628220-2] Choosing cybersecurity risk identification and assessment approaches for critical infrastructure: A background exploration and pilot study proposal
REFERENCE #:	
SUBMISSION TYPE:	Amendment/Modification
ACTION:	APPROVED
APPROVAL DATE:	February 24, 2021
EXPIRATION DATE:	December 9, 2021
REVIEW TYPE:	Expedited Review
REVIEW CATEGORY:	Expedited review category # 7. Waiver of Written Consent (For Oral Consent): 45CFR46.117(c)(1) applies.

Thank you for your submission of Amendment/Modification materials for this project. The University of Maryland College Park (UMCP) IRB has APPROVED your submission. This approval is based on an appropriate risk/benefit ratio and a project design wherein the risks have been minimized. All research must be conducted in accordance with this approved submission.

Prior to submission to the IRB Office, this project received scientific review from the departmental IRB Liaison.

This submission has received Expedited Review based on the applicable federal regulations.

This project has been determined to be a MINIMAL RISK project. Based on the risks, this project requires continuing review by this committee on an annual basis. Please use the appropriate forms for this procedure. Your documentation for continuing review must be received with sufficient time for review and continued approval before the expiration date of December 9, 2021.

Please remember that informed consent is a process beginning with a description of the project and insurance of participant understanding followed by a signed consent form. Informed consent must continue throughout the project via a dialogue between the researcher and research participant. Unless a consent waiver or alteration has been approved, Federal regulations require that each participant receives a copy of the consent document.

Please note that any revision to previously approved materials must be approved by this committee prior to initiation. Please use the appropriate revision forms for this procedure.

All UNANTICIPATED PROBLEMS involving risks to subjects or others (UPIRSOs) and SERIOUS and UNEXPECTED adverse events must be reported promptly to this office. Please use the appropriate reporting forms for this procedure. All FDA and sponsor reporting requirements should also be followed.

All NON-COMPLIANCE issues or COMPLAINTS regarding this project must be reported promptly to this office.

Please note that all research records must be retained for a minimum of seven years after the completion of the project.

If you have any questions, please contact the IRB Office at 301-405-4212 or irb@umd.edu. Please include your project title and reference number in all correspondence with this committee.

This letter has been electronically signed in accordance with all applicable regulations, and a copy is retained within University of Maryland College Park (UMCP) IRB's records.

UNIVERSITY OF MARYLAND
INSTITUTIONAL REVIEW BOARD

1204 Marie Mount Hall
College Park, MD 20742-5125
TEL 301.405.4212
FAX 301.314.1475
irb@umd.edu
www.umresearch.umd.edu/IRB

DATE:	November 17, 2021
TO:	Shawn Janzen
FROM:	University of Maryland College Park (UMCP) IRB
PROJECT TITLE:	[1628220-3] Choosing cybersecurity risk identification and assessment approaches for critical infrastructure: A background exploration and pilot study proposal
SUBMISSION TYPE:	Continuing Review/Progress Report
ACTION:	APPROVED
APPROVAL DATE:	November 17, 2021
REVIEW TYPE:	Expedited Review
REVIEW CATEGORY:	Expedited review category #7. Waiver of documentation of consent under 45CFR46.117(c)

Thank you for your submission of Continuing Review/Progress Report materials for this project. The University of Maryland College Park (UMCP) IRB has APPROVED your submission. This approval is based on an appropriate risk/benefit ratio and a project design wherein the risks have been minimized. All research must be conducted in accordance with this approved submission.

Prior to final approval of this project scientific review was completed by the IRB Member reviewer.

This submission has received Expedited Review based on the applicable federal regulations.

This project has been determined to be a MINIMAL RISK project.

Please remember that informed consent is a process beginning with a description of the project and insurance of participant understanding followed by a signed consent form. Informed consent must continue throughout the project via a dialogue between the researcher and research participant. Unless a consent waiver or alteration has been approved, Federal regulations require that each participant receives a copy of the consent document.

Please note that any revision to previously approved materials must be approved by this committee prior to initiation. Please use the appropriate Amendment forms for this procedure.

All UNANTICIPATED PROBLEMS involving risks to subjects or others (UPIRSOs) and SERIOUS and UNEXPECTED adverse events must be reported promptly to this office. Please use the appropriate reporting forms for this procedure. All FDA and sponsor reporting requirements should also be followed. All NON-COMPLIANCE issues or COMPLAINTS regarding this project must be reported promptly to this office.

Please note that all research records must be retained for a minimum of seven years after the completion of the project.

This letter has been electronically signed in accordance with all applicable regulations, and a copy is retained within University of Maryland College Park (UMCP) IRB's records.

UNIVERSITY OF MARYLAND
INSTITUTIONAL REVIEW BOARD

1204 Marie Mount Hall
College Park, MD 20742-5125
TEL 301.405.4212
FAX 301.314.1475
irb@umd.edu
www.umresearch.umd.edu/IRB

DATE:	November 15, 2022
TO:	Shawn Janzen
FROM:	University of Maryland College Park (UMCP) IRB
PROJECT TITLE:	[1628220-4] Choosing cybersecurity risk identification and assessment approaches for critical infrastructure
SUBMISSION TYPE:	Amendment/Modification
ACTION:	APPROVED
APPROVAL DATE:	November 15, 2022
REVIEW TYPE:	Expedited Review
REVIEW CATEGORY:	Expedited review category # *7, Waiver of Consent Documentation 45 CFR 46.117(c)*

Thank you for your submission of Amendment/Modification materials for this project. The University of Maryland College Park (UMCP) IRB has APPROVED your submission. This approval is based on an appropriate risk/benefit ratio and a project design wherein the risks have been minimized. All research must be conducted in accordance with this approved submission.

Prior to final approval of this project scientific review was completed by the IRB Member reviewer.

This submission has received Expedited Review based on the applicable federal regulations.

This project has been determined to be a MINIMAL RISK project.

Please remember that informed consent is a process beginning with a description of the project and insurance of participant understanding followed by a signed consent form. Informed consent must continue throughout the project via a dialogue between the researcher and research participant. Unless a consent waiver or alteration has been approved, Federal regulations require that each participant receives a copy of the consent document.

Please note that any revision to previously approved materials must be approved by this committee prior to initiation. Please use the appropriate Amendment forms for this procedure.

All UNANTICIPATED PROBLEMS involving risks to subjects or others (UPIRSOs) and SERIOUS and UNEXPECTED adverse events must be reported promptly to this office. Please use the appropriate reporting forms for this procedure. All FDA and sponsor reporting requirements should also be followed. All NON-COMPLIANCE issues or COMPLAINTS regarding this project must be reported promptly to this office.

Please note that all research records must be retained for a minimum of seven years after the completion of the project.

If you have any questions, please contact the IRB Office at 301-405-4212 or irb@umd.edu. Please include your project title and reference number in all correspondence with this committee.

This letter has been electronically signed in accordance with all applicable regulations, and a copy is retained within University of Maryland College Park (UMCP) IRB's records.

Appendix F: Full Size Charts from Chapter 5

Table 43

Manger Certifications: Risk Management and/or Cybersecurity

Certification	Int. N	Sur. N	Full Certification Name	Certifying Organization
CISSP	10	89	Certified Information Systems Security Professional	(ISC)^2
CISA	2	37	Certified Information Systems Auditor	ISACA
CISM	3	27	Certified Information Security Manager	ISACA
CEH	3	18	Certified Ethical Hacker	EC-Council
CRISC	1	15	Certification in Risk and Information Systems Control	ISACA
Security+	1	15	Security+	CompTIA
CGEIT	1	8	Certified Governance of Enterprise IT	ISACA
CDPSE		8	Certified Data Privacy Solutions Engineer	ISACA
SSCP		8	Systems Security Certified Practitioner	(ISC)^2
GSEC		7	Global Information Assurance Certification (GIAC) Security Essentials	SANS Institute
PMP	3	4	Project Management Professional	Project Management Institute (PMI)
Executive	6		*	*
CRMP		5	Certified Risk Management Professional	Risk and Insurance Management Society (RIMS)
RMP		4	Risk Management Professional	Project Management Institute (PMI)
CASP		3	CompTIA Advanced Security Practitioner	CompTIA
GCIH	1	2	Global Information Assurance Certification (GIAC) Certified Incident Handler	SANS Institute
OSCP		3	Offensive Security Certified Professional	Offensive Security

Certification	Int. N	Sur. N	Full Certification Name	Certifying Organization
AWS	1		AWS Certified Security	Amazon
CAPM	1		Certified Associate in Project Management	Project Management Institute (PMI)
CASE		1	Certified Application Security Engineer	EC-Council
CCNA	1		Cisco Certified Network Associate	Cisco
CCNP	1		Cisco Certified Network Professional	Cisco
CCP	1		Certified Cloud Practitioner	Amazon
CCSP		1	Certified Agile Service Manager (CASM)	DevOps Institute
CEI	1		Certified EC-Council Instructor	EC-Council
CENA		1	**	**
CMMC	1		Cybersecurity Maturity Model Certification Registered Professional	CMMC Accreditation Body
CPT	1		Certified Penetration Tester	**
CRM		1	Certified Risk Manager	The National Alliance for Insurance Education & Research
CSEP		1	Certified Systems Engineering Professional	INCOSE
CSX	1		Cybersecurity Nexus	ISACA
CWNA	1		Certified Wireless Network Administrator	Certified Wireless Network Professional
ECSA	1		EC-Council Certified Security Analyst	EC-Council
FAIR	1		FAIR (Factor Analysis of Information Risk) Pracitioner	FAIR Institute
IAM	1		Identity and Access Management	**
ITIL	1		Information Technology Infrastructure Library	Axelos
LPT	1		Licensed Penetration Tester	EC-Council
MCSE	1		Microsoft Certified Systems Engineer	Microsoft
NCSS		1	Nortel Certified Support Specialist	Nortel Networks Corporation
SSCP	1		Systems Security Certified Practitioner	(ISC)^2

** Self-identified, not mutually exclusive*

*** Unclear if a risk management or cybersecurity certification; CENA seems related to nursing*

Table 44

Heatmap Table of Approaches and Traits (Full)

1 of 6 **Approaches ➔** **Binary Traits ⬇**	CIS 18/ CSC	CMMC	CMMI	COBIT	Custom	FAIR	ISO-27001/2	ISO-27005	ISO-31000	MITRE ATT&CK	MITRE Shield	NIST CSF	NIST SP 800-171	NIST SP 800-30	NIST SP 800-37	NIST SP 800-39	NIST SP 800-53	NIST SP 800-82	NISTIR 8286	OCTAVE	PHA	SCF	SOC-C
Mgr AICPA Famliarity	15	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Approach Process: Board Involved	0	0	0	2	0	0	0	1	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0
Mgr Approach Process: Consultant (as Fundamental Framework Role)	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Approach Process: C-Suite Involved	1	0	0	23	0	0	2	0	0	0	0	2	0	0	0	0	0	3	0	0	0	0	9
Mgr Approach Process: External Consultants	8	4	0	14	0	0	2	0	0	5	0	0	0	19	0	0	1	2	0	0	0	0	22
Mgr Approach Process: Internal Consultation	0	0	0	4	0	0	1	1	0	11	0	1	6	0	7	9	0	13	5	0	29	0	8
Mgr Construct: Company Output Quality > Average	2	0	0	5	0	0	2	7	34	0	9	2	14	0	5	26	5	2	0	0	16	15	0
Mgr Construct: Company's Privce Value > Average	2	4	0	5	29	0	5	8	1	2	16	2	4	0	0	9	2	11	0	0	2	19	0
Mgr Construct: Cyber Insurance Requirements > Average	1	1	0	5	22	4	4	2	13	5	0	2	0	0	6	0	4	8	0	0	10	5	10
Mgr Construct: Facilitating Conditions > Average	3	0	0	5	0	0	4	14	1	1	0	0	2	0	5	25	5	29	3	0	16	21	0
Mgr Construct: Hedonic Motivation > Average	0	0	0	5	0	0	4	15	8	0	9	1	8	0	5	24	5	0	0	0	1	0	0
Mgr Construct: Social Influence > Average	5	0	0	2	0	0	6	14	2	1	0	3	11	23	5	8	4	0	3	12	20	13	0
Mgr Degree Major: Business	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Degree Major: Computer Science / IT	5	8	0	5	42	11	6	15	0	15	0	3	5	0	8	0	4	0	0	0	12	3	15
Mgr Degree Major: Engineering	0	0	0	0	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0	0	0	0	0
Mgr Degree Major: Information / Data Science	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2 of 6 Approaches ➔ Binary Traits ➔	CIS 18/ CSC	CMMC	CMMI	COBIT	Custom	FAIR	ISO-27001/2	ISO-27005	ISO-31000	MITRE ATT&CK	MITRE Shield	NIST CSF	NIST SP 800-171	NIST SP 800-30	NIST SP 800-37	NIST SP 800-39	NIST SP 800-53	NIST SP 800-82	NISTIR 8286	OCTAVE	PHA	SCF	SOC-C
Mgr Encounter Approaches: Generally Keep Informed	6	22	25	5	37	28	2	3	9	5	37	7	37	14	0	27	10	35	0	0	14	16	9
Mgr Encounter Approaches: Learn When Necessary	0	0	0	1	0	0	2	2	0	2	0	1	0	0	0	0	0	0	0	0	0	0	2
Mgr Highest Degree: Associate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0
Mgr Highest Degree: Bachelor	5	0	0	0	16	0	5	7	14	0	14	2	0	0	0	24	2	4	0	0	0	15	17
Mgr Highest Degree: Masters	2	26	12	1	0	11	0	0	0	5	0	0	7	0	6	0	1	0	0	0	0	0	0
Mgr IT / OT Challenges with approach selection: Lack of Good Approaches for OT / CPS.	0	0	1	0	29	0	0	0	0	1	0	0	0	0	0	0	0	26	0	0	0	0	0
Mgr IT / OT Challenges with approach selection: No Selection Challenges	1	0	0	2	0	0	1	1	0	0	0	7	0	0	11	0	0	0	0	0	0	0	0
Mgr IT / OT Challenges with approach selection: Too IT Focused	5	4	7	0	0	0	1	30	13	2	0	0	4	0	0	0	16	0	0	0	0	63	5
Mgr Level: Executive	2	18	95	0	0	68	0	0	0	18	0	0	11	0	0	0	0	0	0	0	0	0	0
Mgr Level: Middle	0	1	0	3	14	0	2	24	29	0	22	3	10	22	7	9	0	0	0	0	14	22	1
Mgr Level: Upper	0	14	0	0	1	0	1	0	0	6	0	6	0	0	0	0	8	2	0	0	0	0	0
Mgr Location: Inside US	0	6	0	5	0	0	3	6	4	0	25	2	0	0	6	0	5	1	0	9	5	5	19
Mgr Location: Multi-National Company w/HQ Inside US	0	0	0	0	0	0	0	0	0	0	0	0	47	0	0	0	0	0	0	0	0	0	0
Mgr Measurement Preferences: Descriptive Scales	4	3	21	0	0	0	1	4	1	12	0	4	8	28	0	40	0	18	0	0	0	7	0
Mgr Measurement Preferences: Explicit Numeric Values	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	6	0	18
Mgr Measurement Preferences: Numeric Scales or Percents	0	45	0	3	0	0	3	2	0	3	0	2	0	0	7	0	3	4	0	0	0	0	15
Mgr Number of Approaches Selected > Average	8	12	19	7	2	28	5	0	0	9	17	11	9	21	5	6	8	37	4	17	4	19	9

3 of 6 Approaches ➔ Binary Traits ➔	CIS 18/ CSC	CMMC	CMMI	COBIT	Custom	FAIR	ISO-27001/2	ISO-27005	ISO-31000	MITRE ATT&CK	MITRE Shield	NIST CSF	NIST SP 800-171	NIST SP 800-30	NIST SP 800-37	NIST SP 800-39	NIST SP 800-53	NIST SP 800-82	NISTIR 8286	OCTAVE	PHA	SCF	SOC-C
Mgr Org Relevant: CIS	0	0	0	36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Org Relevant: CSN	0	0	0	1	0	0	8	0	0	0	0	42	0	0	0	0	0	0	0	0	0	0	0
Mgr Org Relevant: ISA	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Org Relevant: ISACA	3	18	12	0	0	0	0	0	0	28	0	1	0	0	0	0	2	0	0	0	1	0	0
Mgr Org Relevant: ISC^2	0	53	0	0	0	0	1	0	0	11	73	1	0	0	0	0	0	0	0	0	0	26	0
Mgr Org Relevant: ISSA	0	0	0	2	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0
Mgr Org Relevant: NCSS	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Org Relevant: PMI	10	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Mgr Org Relevant: RIMS	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Org Relevant: SANS Institute	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	73	0	0	0	0	0	0
Mgr Orgs Active: AEHIS	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Mgr Orgs Active: CSN	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Orgs Active: ISA	9	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Orgs Active: ISACA	6	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Orgs Active: ISS	0	0	0	48	0	0	22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Orgs Active: ISSA	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Orgs Active: RIMS	1	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Professional Cert.: CDPSE	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	1	0	0	0	0	0	0
Mgr Professional Cert.: CEH	0	0	0	1	0	0	1	0	0	0	0	15	0	0	0	0	1	0	0	0	0	0	0
Mgr Professional Cert.: CGEIT	0	0	0	0	0	0	4	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Professional Cert.: CISA	1	5	0	0	0	0	0	0	6	1	2	2	0	0	0	0	0	0	0	0	0	0	0
Mgr Professional Cert.: CISM	3	5	0	0	0	0	0	0	0	5	0	1	0	0	0	0	0	0	0	0	0	0	0
Mgr Professional Cert.: CISSP	1	8	0	4	0	0	3	16	0	2	0	1	0	0	0	0	3	0	0	0	0	7	0
Mgr Professional Cert.: CRISC	2	0	0	0	0	0	0	0	0	28	0	0	0	0	0	0	0	0	0	0	5	0	0
Mgr Professional Cert.: CRMP	6	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0
Mgr Professional Cert.: GSEC	0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr Professional Cert.: RMP	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0
Mgr Professional Cert.: Security+	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

4 of 6 Approaches ➔ Binary Traits ➔	CIS 18/ CSC	CMMC	CMMI	COBIT	Custom	FAIR	ISO-27001/2	ISO-27005	ISO-31000	MITRE ATT&CK	MITRE Shield	NIST CSF	NIST SP 800-171	NIST SP 800-30	NIST SP 800-37	NIST SP 800-39	NIST SP 800-53	NIST SP 800-82	NISTIR 8286	OCTAVE	PHA	SCF	SOC-C
Mgr Professional Cert.: SSCP	0	0	0	1	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr RI&A Duty Freq.: Choose	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mgr RI&A Duty Freq.: Frequently	2	2	0	0	0	0	1	6	40	3	1	1	11	0	0	0	5	0	0	0	0	0	6
Mgr RI&A Duty Freq.: Perform & Choose	0	4	0	5	32	0	2	9	24	0	20	2	6	0	6	1	5	0	0	6	6	9	7
Mgr RI&A Duty Freq.: Regularly	4	18	29	8	2	28	2	0	0	10	0	7	0	0	0	90	0	38	0	0	0	0	18
Mgr Use Approach for IT or OT: CPS	0	0	0	2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Mgr Use Approach for IT or OT: IT	1	9	0	0	0	0	1	0	0	10	9	0	31	0	0	0	1	4	0	0	0	0	51
Mgr Use Approach for IT or OT: IT & CPS	0	0	0	1	0	0	1	50	0	0	0	0	0	0	15	0	0	0	0	0	0	0	0
Mgr Use Approach for IT or OT: IT & OT	10	6	0	0	0	0	0	0	24	3	0	0	0	0	0	34	18	0	0	0	0	1	0
Mgr Use Approach for IT or OT: IT & OT & CPS	1	2	32	0	69	0	1	0	0	12	0	26	4	0	0	0	1	4	0	0	0	0	0
Mgr Years of Experience: 11-20 years	1	10	0	0	0	0	3	6	0	5	0	2	2	0	0	0	2	0	0	0	17	0	0
Mgr Years of Experience: 21+ years	0	2	64	0	0	59	0	1	0	19	0	4	0	0	0	0	0	12	0	0	0	0	1
Mgr Years of Experience: 6-10 years	4	1	0	0	29	0	1	0	12	1	12	0	0	0	0	12	0	0	0	24	0	0	12
Org Crit. Inf. Sector: Chemical	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0
Org Crit. Inf. Sector: Commercial Facilities	0	0	0	0	2	0	0	0	0	2	0	21	0	0	0	0	17	0	0	0	0	0	0
Org Crit. Inf. Sector: Critical Manufacturing	0	5	0	0	0	0	0	0	63	7	0	2	0	0	0	0	0	0	0	0	0	73	0
Org Crit. Inf. Sector: Defense Industrial Base	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org Crit. Inf. Sector: Energy	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org Crit. Inf. Sector: Food & Agriculture	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8
Org Crit. Inf. Sector: Government Facilities	0	0	0	0	0	0	1	3	0	0	0	0	0	0	51	0	0	0	0	0	0	0	0

5 of 6 **Approaches ➔** **Binary Traits ➔**	CIS 18/ CSC	CMMC	CMMI	COBIT	Custom	FAIR	ISO-27001/2	ISO-27005	ISO-31000	MITRE ATT&CK	MITRE Shield	NIST CSF	NIST SP 800-171	NIST SP 800-30	NIST SP 800-37	NIST SP 800-39	NIST SP 800-53	NIST SP 800-82	NISTIR 8286	OCTAVE	PHA	SCF	SOC-C
Org Crit. Inf. Sector: Healthcare & Public Health	1	0	0	0	0	0	0	8	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Org Crit. Inf. Sector: IT & OT	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Org Crit. Inf. Sector: Transportations Systems	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Org Crit. Inf. Sector: Water & Wastewater Systems	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org Cyberteam work group includes: 3rd Party Accounting & Finance	4	25	0	0	0	0	0	0	0	0	25	0	0	26	0	9	0	0	0	0	0	0	15
Org Cyberteam work group includes: Accounting & Finance	5	3	16	15	1	26	2	7	14	7	0	5	34	1	6	0	4	1	0	11	10	14	1
Org Cyberteam work group includes: Does not work with Accounting & Finance	1	0	0	0	0	0	5	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0
Org ISAC Membership: ACC	1	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	90	0	0
Org ISAC Membership: AUTO	1	0	0	0	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	0	0	0	0
Org ISAC Membership: Health	1	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org ISAC Membership: HealthcareReady	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org ISAC Membership: IT	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	0	0
Org ISAC Membership: National Defense	0	0	0	0	0	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0	0	0	0
Org ISAC Membership: Oil & Natural Gas	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org ISAC Membership: Real Estate	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0
Org ISAC Membership: Research	0	0	0	1	0	0	1	0	0	0	0	0	0	0	59	0	0	0	0	0	0	0	0
Org ISAC Membership: Surface Transportation	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org ISAC Membership: Water	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org Outsourcing CS RI&A: Cybersecurity	3	0	0	0	0	0	0	78	0	6	0	0	0	0	0	0	1	0	0	0	0	0	0

6 of 6 **Approaches ➔** **Binary Traits ➔**	CIS 18/ CSC	CMMC	CMMI	COBIT	Custom	FAIR	ISO-27001/2	ISO-27005	ISO-31000	MITRE ATT&CK	MITRE Shield	NIST CSF	NIST SP 800-171	NIST SP 800-30	NIST SP 800-37	NIST SP 800-39	NIST SP 800-53	NIST SP 800-82	NISTIR 8286	OCTAVE	PHA	SCF	SOC-C
Org Outsourcing CS RI&A: Cybersecurity + Risk Identification & Assessment	1	0	24	17	0	9	3	0	0	9	0	3	0	4	8	0	2	4	0	0	0	23	20
Org Outsourcing CS RI&A: Risk Identification & Assessment	1	0	0	0	0	0	0	7	0	1	0	0	7	0	0	0	0	0	0	0	0	0	0
Org Size: 10-100 people	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org Size: 101-1,000 people	1	5	3	0	0	0	2	10	0	2	37	0	2	0	0	0	2	17	0	0	75	0	23
Org Size: 1,000 - 10,000 people	1	10	0	1	0	0	0	3	1	5	0	0	30	0	85	5	0	0	0	0	0	0	0
Org Size: 10,000 - 25,0000 people	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Org Size: For-Profit	2	27	8	2	20	43	3	4	31	0	20	5	18	20	0	19	3	36	4	7	7	11	27
Org Size: Non-Profit	2	0	0	1	0	0	1	0	0	0	0	2	3	0	25	0	0	0	0	0	0	0	0
Org Size: Private	4	9	9	2	21	9	2	2	5	2	31	5	10	4	0	7	4	23	0	7	6	2	30
Org Size: Public	0	0	0	0	0	0	0	3	22	0	0	0	6	0	0	0	0	0	0	0	0	0	0

Glossary

This paper bridges several branches of disciplinary research, practice, and their terms of art. To avoid confusion within and between them, this glossary includes the following terms: public, cybersecurity, risk, risk management, CSR managers, critical infrastructure, and approaches.

Approaches. I define approaches as the rich range of diverse options to help understand risk identification and assessment which include methods, models, frameworks, guidance, and procedures. Approaches represent the complexity, innovation, and level of analytical engagement of risk identification and assessment for cybersecurity and critical infrastructure. I choose to group approaches broadly rather focus on one or a subset of the options for two reasons. First, individually the options vary in their ability to measure and explain risk to meet particular use case designs and other needs (Giannopoulous et al., 2012). For example, focusing only on assessment designs like vulnerability interdependencies (Zio & Sansavini, 2011), or software like Better Infrastructure Risk and Resilience (BIRR) (Sagoff, 2010), imposes constraints on what and how risk measurements occur and are calculated as well as the type and level of expert knowledge required to engage that approach.

Second, building on the prior reason, it is yet unclear what or which options CSR managers use and approaches are not mutually exclusive; therefore, I must allow for some amount of mixed approach use. This is potentially due to frequently observed separation of key guidelines from the implementation instructions to meet those guidelines. For example, guidance for managing cybersecurity ambiguously often refers to best practices, but such practices refer to a quality-based selector of how to work and not provide concrete examples of those practices. The ambiguity allows flexibility for a range of cybersecurity risk identification and assessment needs and use cases. Thus, pairing between these types of approaches may occur.

Critical infrastructure. I adopt NIST's definition for critical infrastructure as the "system and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (2013, p.B-3). I chose this version over its predecessor from the US President's Commission on Critical Infrastructure Protection (PCCIP) (1997) because of specific inclusion for public health and safety. Trends in the literature tend to use critical infrastructure without definition (Bairdi, Telmon, & Sgandurra, 2009; Slayton & Clark-Ginsbert, 2018) or use a near identical definition without the US-specific context (Herrera & Maennel, 2019), but usage does not differ much.

Cyber incident. Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. (NIST SP 800-160 Vol. 2 Rev. 1)

Cyber-physical system. Informational technologies (IT) and operational technologies (OT) integrated into common systems that span digital and physical spaces.

Cybersecurity. I define cybersecurity as the actions and ability to protect or defend the use of cyberspace and the technologies, people, and data that access cyberspace from cyber events and

other forms of impactful technological failure. I blended the definitions from National Institute of Standards and Technology (NIST) (2012), Harry (2018), and Agresti (2010) to expand the depth of NIST's and Harry's definitions of operational cyberspace and unauthorized cyber events to be more inclusive and include Agresti's more holistic view on the organization.
The NIST SP 800-30 defined view of cybersecurity applies a militaristic tone layered onto the protection of information environments and infrastructure, framed as a potential battlefield with attack vectors (2015). Harry (2018) discussed cyber events on network security, as the resulting effects of unauthorized maneuvers against networks and related technologies. Harry (2018) use of network security is analogous to NIST's positioning of cybersecurity as a protective front against cyber-attacks.

NIST and Harry's use of cybersecurity as the chess match-esque strategy against an antagonistic actor was but one vector in the spectrum of security threats. A more holistic definition of cybersecurity should consider the advent of technological failure caused by humans that do not mean harm, such as an internal employee that accidentally breaks a component, and by non-human means such as components that naturally wear out.
Agresti (2010) painted cybersecurity more as a strategic and transformational exercise, most simply understood as a rebranding with the cyber- prefixture to denote its digital environment. He also positioned it as a domain of national defense but one that is invisible compared to the physical domains.

Cybersecurity risk managers. I define CSR managers as those who operate, make decisions regarding, and otherwise implement governance and policy of risk management toward cybersecurity. While general implementation may pertain to risk management broadly, CSR managers spend at least part of that effort on some aspects of cyber risk identification and assessment. Using management as a typology allows for three vertical tiers, where the lowest level of CSR managers is the front-line professionals who apply cybersecurity actions to information technology (IT) and operational technology (OT). A middle tier consists of management professionals that manage the human and technical cybersecurity systems, including the first-tier managers. The highest tier comprises managers of CSR governance, including regulation and oversight. For this study, I refer to all CSR managers as a common group except when specifically mentioned. Characteristics such as years of experience may allow mobility between tiers and organizational mandates may place CSR managers in more than one tier with operational duties that are both technical and bureaucratic. Therefore, my definition of CSR managers is wide during this exploratory study to accommodate the nuanced differences between types of managers. To address the grey spaces where public lines blur with various types of partnerships and contracts, public CSR managers include those professionals working within government; I do not include those working on behalf of government, even if that work is on or for public cybersecurity issues. I make this distinction based on nuanced differences between public and private, particularly when it comes to matters of political control, accountability, and transparency. I discuss additional distinctions in the methods section below.

Information environment. "The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." (Joint Chiefs of Staff, 2014)

Public. I limit that the public sector, or just public, means government and not nonprofits or civil society. It may pertain to government at any level, and I will specify the level of government if necessary at that time. I set this limit because governments possess national security responsibilities and authority that nonprofits and civil society do not, which can affect organizational goal-setting and policy process (Ferwerda, Chouchi, & Madnick, 2010).

Risk. I start with NIST's definition of risk as a function of event impact and probability of the event happening but broaden what they call "adverse impacts" (2012, p.B-19) into what the US Department of Homeland Security (DHS) calls "unwanted outcomes" (DHS S&T, 2018, p.2) because not all events are adverse. I align this definition within the same context of NIST's information system-related security risk "to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems" (2012, p.B-19).
My adapted core definition of risk is streamlined--only regarding risk as computational elements that determine the threat measure, while the information system security frame provides a boundary. Other definitions of risk across the literature range in their congruence with NIST or DHS definitions but are rarely as succinct. The fractured agreement in defining a single word term reveals some disciplinary boundaries, and conceptions of what is important to understand security and risk. It reinforces the notion that while users of a term may adopt its use, they understand and frame it differently. This idea has supporting implications later when I introduce my conceptual framework.

Risk management. I adapt NIST's definition for a cybersecurity risk context including "organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation" and apply the four simplified stages of identify, assess, manage, and evaluate as displayed in Figure *21* after taking into account commonalities shared with other definitions of risk (2012, p.B-19). I align with NIST's view of risk management because it is framed within information security, highly detailed in scope, and yet relatively compact. However, compared to several other definitions, NIST is not explicit about an identification stage, which I believe is embedded as part of context and assessment. My focus on both identification and assessment reflects how some approaches do not delineate them as separate stages. Other definitions generally reflect high level concepts of risk and tend to overlap. I emulate their typical process-oriented cyclical stages in Figure *21*.

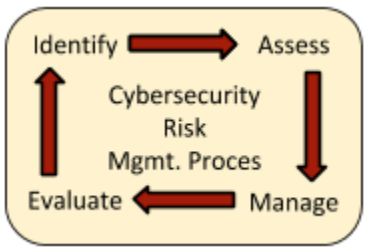


Figure 26: A Simplified Risk Management Cycle for Cybersecurity

Technology. I operationalize technology drawing upon Rogers' (2003) view of technology as having a software aspect, "consisting of the information base for the tool [...] and [the software] consisting of the coded commands, instructions, manuals, and other information aspects [...] for certain tasks" (p.13). Some approaches may fit cleanly into this definition, such as the actual software solutions like BIRR (Sagoff, 2010), while others like the NIST RMF, OCTAVE, and FAIR as frameworks appear less so. However, I take the position that frameworks and similar approaches contain instructions and other information aspects to complete risk identification and

assessment tasks. This may pass muster with an innovation scholar or science and technology philosopher, but not as well for someone familiar with the Technology Adoption Model (TAM3) or who might not equate the ideas and objects of innovation as equivalent to the instruments of technology (Venkatesh & Davis, 2008).

Therefore, I reframe how theories referencing technology can be used specifically for the decision- making activity as the key. In this context, technology is important, but it takes second priority to the selection action of choosing the technology; for example, TAM3 has a usefulness in that it takes context heavily into account as to why someone would adopt a technology but does poorly in predicting future usage. However, TAM3 contains core instruments that are clearly broken down, well defined, and validated over numerous studies (ibid.; Hilmer, 2009). I use TAM3's core instruments as thought aids to assess why an approach understood as technology is selected.

Bibliography

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Agresti, W. W. (2010). The Four Forces Shaping Cybersecurity. *Computer*, *43*(2), 101–104. https://doi.org/10.1109/MC.2010.53

Aguinis, H., Forcum, L. E., & Joo, H. (2013). Using Market Basket Analysis in Management Research. *Journal of Management*, *39*(7), 1799–1824. https://doi.org/10.1177/0149206312466147

Alberts, C. J., Dorofee, A. J., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE Approach*. Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/UsersGuide/2003_012_001_51556.pdf

Allen, T. J., Tushman, M. L., & Lee, D. M. S. (1979). Technology Transfer as a Function of Position in the Spectrum from Research Through Development to Technical Services. *Academy of Management Journal*, *22*(4), 694–708. https://doi.org/10.5465/255809

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Amirkhanyan, A. A., Meier, K. J., O'Toole, L. J., Jr., Dakhwe, M. A., & Janzen, S. (2018). Management and Performance in US Nursing Homes. *Journal of Public Administration Research and Theory*, *28*(1), 33–49. https://doi.org/10.1093/jopart/mux003

Ani, U. D., Watson, J. D. McK., Nurse, J. C., Cook, A., & Maple, C. (2019, May 1). A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. *Living in the Internet of Things (IoT 2019)*. PETRAS/IET Conference, London, UK. https://digital-library.theiet.org/content/conferences/10.1049/cp.2019.0131

Abu, M. S., Ariffin, A., Selamat, S. R., & Yusof, R. (2021). Formulation of Association Rule Mining (ARM) for an Effective Cyber Attack Attribution in Cyber Threat Intelligence (CTI). *International Journal of Advanced Computer Science and Applications*, *12*(4), 134–143. https://d1wqtxts1xzle7.cloudfront.net/99298967/Paper_18-Formulation_of_Association_Rule_Mining-libre.pdf

Aspen Tech Policy Hub. (2021). *Diversity, Equity, and Inclusion in Cybersecurity*. Aspen Tech Policy Hub. https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf

Atkins, S., & Lawson, C. (2021). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review*, *81*(5), 847–861. https://doi.org/10.1111/puar.13322

Auerswald, P., Branscomb, L. M., La Porte, T. M., & Michel-Kerjan, E. (2005). The Challenge of Protecting Critical Infrastructure. *Issues in Science and Technology*, *22*(1), 77–83. https://www.jstor.org/stable/43314287

Bigueur, M. (2015, August 2). Risk Analysis Management and Methodology. *Bigueur's Blogosphere*. https://miguelbigueur.com/2015/08/02/risk-assessment-methodologies/

Bohte, J., & Meier, K. J. (2000). Goal Displacement: Assessing the Motivation for Organizational Cheating. *Public Administration Review*, *60*(2), 173–182. https://doi.org/10.1111/0033-3352.00075

Boiral, O. (2003). ISO 9000: Outside the Iron Cage. *Organization Science*, *14*(6), 720–737. https://doi.org/10.1287/orsc.14.6.720.24873

Bretschneider, S. (1990). Management Information Systems in Public and Private Organizations: An Empirical Test. *Public Administration Review*, *50*(5), 536–545. JSTOR. https://doi.org/10.2307/976784

Bretschneider, S. I., & Mergel, I. (2011). Technology and public management information systems. In D. C. Menzel & J. D. White (Eds.), *The state of public administration: Issues, challenges, and opportunities* (pp. 187–203). Routledge; https://www.routledge.com/The-State-of-Public-Administration-Issues-Challenges-and-Opportunities/Menzel-White/p/book/9780765625052

Brühlmann, F., Petralito, S., Aeschbach, L. F., & Opwis, K. (2020). The quality of data collected online: An investigation of careless responding in a crowdsourced sample. *Methods in Psychology*, *2*, 100022. https://doi.org/10.1016/j.metip.2020.100022

Burch, G. F., Burch, J., & McGarry, M. (2024). Cybersecurity Risk Management Governance: An Agency Theory Perspective. *ISACA Journal*, *5*. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-5/cybersecurity-risk-management-governance

Campagna, J. M., & Bhada, S. V. (2024). Strategic Adoption of Digital Innovations Leading to Digital Transformation: A Literature Review and Discussion. *Systems*, *12*(4), 118. https://doi.org/10.3390/systems12040118

Campbell, M. (2022, February 17). GoTech receives competitive TEDCO grant for TAPESTRY program. *University of Maryland School of Public Policy*. https://spp.umd.edu/news/gotech-receives-competitive-tedco-grant-tapestry-program

Capterra. (n.d.). *Best Risk Management Software 2020 | Reviews of the Most Popular Tools & Systems*. https://www.capterra.com/risk-management-software/

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process* (CMU/SEI-2007-TR-012). Software Engineering Institute. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

Carminati, L. (2018). Generalizability in Qualitative Research: A Tale of Two Traditions. *Qualitative Health Research*, *28*(13), 2094–2101. https://doi.org/10.1177/1049732318788379

Cassell, C., & Symon, G. (2004). *Essential Guide to Qualitative Methods in Organizational Research*. https://doi.org/10.4135/9781446280119

Caudle, S. L., Gorr, W. L., & Newcomer, K. E. (1991). MIS Quarterly. *MIS Quarterly*, *15*(2), 171–188. https://doi.org/10.2307/249378

Chambliss, A. (2025). *Cybersecurity in 2025: What CISOs in Retail & Hospitality Are Prioritizing—RH-ISAC* (CISO Benchmark). Retail & Hospitality ISAC. https://rhisac.org/reports/cybersecurity-in-2025-what-cisos-in-retail-hospitality-are-prioritizing/

Charmaz, K. (2005). Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis. SAGE. https://www.google.com/books/edition/Constructing_Grounded_Theory/v1qP1KbXz1AC?hl=en&gbpv=0

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Cho, S. Y., Happa, J., & Creese, S. (2020). Capturing Tacit Knowledge in Security Operation Centers. *IEEE Access*, *8*, 42021–42041. https://doi.org/10.1109/ACCESS.2020.2976076

Christensen, C. M., & Overdorf, M. (2000, March 1). Meeting the Challenge of Disruptive Change. *Harvard Business Review*, *March–April 2000*. https://hbr.org/2000/03/meeting-the-challenge-of-disruptive-change

Christopher, J. D., & Lee, A. (2013). *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology* (Technical Update No. 3002001181). Electric Power Research Institute. https://www.energy.gov/sites/prod/files/2014/05/f15/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology_1.pdf

CISCO. (2025). *Cisco Cyber Threat Trends Report*. Cisco. https://www.cisco.com/c/en/us/products/security/cyber-threat-trends-report.html

Clark-Ginsberg, A., & Slayton, R. (2018). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, *46*(3), 339–346. https://doi.org/10.1093/scipol/scy061

Clement, J. (2020, January 17). *Number of cyber security incident reports by federal agencies in the United States from FY 2006 to 2018*. Statistica. https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/

Congressional Research Service. (2019). *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress* (No. R45809). Congressional Research Service. https://fas.org/sgp/crs/homesec/R45809.pdf

Corbin, J., & Strauss, A. (2014). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (4th ed.). SAGE Publications. https://us.sagepub.com/en-us/nam/basics-of-qualitative-research/book235578

Cyberspace Solarium Commission. (2020). *Cyberspace Solarium Commission Report*. Cyberspace Solarium Commission. https://sites.google.com/solarium.gov/cyberspace-solarium-commission

Dasta, V. (2019, February 21). Cyber Risk Assessment: Moving Past the "Heat Map Trap." The Protiviti View. https://blog.protiviti.com/2019/02/21/cyber-risk-assessment-moving-past-the-heat-map-trap/

Decision Point Analytics. (2018, September 27). *Tapestry*. Decision Point Analytics. https://www.decisionpointanalytics.com/tapestry/

DeHart-Davis, L. (2009). Green Tape: A Theory of Effective Organizational Rules. *Journal of Public Administration Research and Theory*, *19*(2), 361–384. https://doi.org/10.1093/jopart/mun004

Deloitte, & National Association of State Chief Information Officers. (2016). *2016 Deloitte-NASCIO Cybersecurity Study—States governments at risk: Turning strategy and awareness into progress*. Deloitte Insights. https://www2.deloitte.com/content/dam/insights/us/articles/3470_2016-Deloitte-NASCIO-cybersecurity-study/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf

Deloitte, & National Association of State Chief Information Officers. (2018). *2018 Deloitte-NASCIO Cybersecurity Study - States at Risk: Bold Plays for Change*. Deloitte Insights. https://www.nascio.org/resource-center/resources/2018-deloitte-nascio-cybersecurity-study-states-at-risk-bold-plays-for-change/

Deloitte, & National Association of State Chief Information Officers. (2020). *2020 Deloitte-NASCIO Cybersecurity Study—States at risk: The cybersecurity imperative in uncertain times*. Deloitte Insights. https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf

Denison, A. J. (2022). *Prevalence and Predictors of Careless Responding in Experience Sampling Research* [Masters thesis, University of South Florida]. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=10538&context=etd

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method, 4th Edition | Wiley* (4th ed.). Wiley. https://www.wiley.com/en-us/Internet%2C+Phone%2C+Mail%2C+and+Mixed+Mode+Surveys%3A+The+Tailored+Design+Method%2C+4th+Edition-p-9781118456149

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147–160. JSTOR. https://doi.org/10.2307/2095101

Dino, L. (2022, May 1). Association mining—Support, Association rules, and Confidence. *Medium*. https://medium.com/@24littledino/association-mining-support-association-rules-and-confidence-60132a37e355

Dotan, R., Blili-Hamelin, B., Madhavan, R., Matthews, J., & Scarpino, J. (2024). *Evolving AI Risk Management: A Maturity Model based on the NIST AI Risk Management Framework* (No. arXiv:2401.15229). arXiv. https://doi.org/10.48550/arXiv.2401.15229

Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review*, *July 2013: Cybersecurity*, 6–11. https://timreview.ca/article/700

Dupuis, M., Meier, E., & Cuneo, F. (2019). Detecting computer-generated random responding in questionnaire-based data: A comparison of seven indices. *Behavior Research Methods*, *51*(5), 2228–2237. https://doi.org/10.3758/s13428-018-1103-y

Dunn, A. M., Heggestad, E. D., Shanock, L. R., & Theilgard, N. (2018). Intra-individual Response Variability as an Indicator of Insufficient Effort Responding: Comparison to Other Indicators and Relationships with Individual Differences. *Journal of Business and Psychology*, *33*(1), 105–121. https://doi.org/10.1007/s10869-016-9479-0

European Union Agency for Cybersecurity, (ENISA). (n.d.). *Inventory of Risk Management / Risk Assessment Methods and Tools* [Page]. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/inventory-of-risk-management-risk-assessment-methods-and-tools

Executive Order 13636. (2013). *Improving Critical Infrastructure Cybersecurity* (Executive Order 78 FR 11737; Federal Register Vol. 78 No. 33, pp. 11737–11744). White House. https://www.federalregister.gov/documents/2001/10/18/01-26509/critical-infrastructure-protection-in-the-information-age

Executive Order 13800. (2017). *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (Executive Order 82 FR 22391; Federal Register Vol. 82 No. 93, pp. 22391–22397). White House. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

Ferwerda, J., Choucri, N., & Madnick, S. (2010). *Institutional foundations for cyber security: Current responses and new challenges* (No. CISL-2009-003). Massachusetts Institute of Technology. https://apps.dtic.mil/docs/citations/ADA530584

Fowler, F. J. (2013). *Survey Research Methods* (Fifth edition). SAGE Publications, Inc. https://www.google.com/books/edition/Survey_Research_Methods/WM11AwAAQBAJ

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology & Health*, *25*(10), 1229–1245. https://doi.org/10.1080/08870440903194015

Freund, J., & Jones, J. (2014). *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann. https://www.amazon.com/Measuring-Managing-Information-Risk-Approach/dp/0124202314

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

Gerstein, D. M., Kallimani, J. G., Mayer, L. A., Meshkat, L., Osburg, J., Davis, P. K., Cignarella, B., & Grammich, C. A. (2016). *Developing a Risk Assessment Methodology for the National Aeronautics and Space Administration:* (No. RR1537). RAND Corporation. https://www.rand.org/pubs/research_reports/RR1537.html

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art* (EUR 25286 EN-2012). European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf

Gilbert, C., & Gilbert, M. A. (2024). Cybersecurity Risk Management Frameworks for Critical Infrastructure Protection. *International Journal of Research Publication and Reviews*, *5*(12), 507–533. https://ijrpr.com/uploads/V5ISSUE12/IJRPR36078.pdf

Goel, R., Haddow, J., & Kumar, A. (2018). *Managing Cybersecurity Risk in Government: An Implementation Model*. IBM Center for The Business of Government. http://www.businessofgovernment.org/sites/default/files/Managing%20Cybersecurity%20Risk%20in%20Government.pdf

Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121–125. https://doi.org/10.1145/1107458.1107465

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*, *09*(02), 133. https://doi.org/10.4236/jis.2018.92010

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, *07*(02), 49. https://doi.org/10.4236/jis.2016.72004

Greer, C., Burns, M. J., Wollman, D. A., & Griffor, E. R. (2019). *Cyber-Physical Systems and Internet of Things* (NIST Pubs No. 1900–202). NIST. https://www.nist.gov/publications/cyber-physical-systems-and-internet-things

Grossmann, M. (2012). Interest group influence on US policy change: An assessment based on policy history. *Interest Groups & Advocacy*, *1*(2), 171–192. https://doi.org/10.1057/iga.2012.9

Gulick, L. (1937). Notes on the Theory of Organization. In L. Gulick & L. Urwick (Eds.), *Papers on the Science of Administration* (pp. 3–13). Blackwell Publishing. https://www.google.com/books/edition/_/YFUiAQAAIAAJ?hl=en&sa=X&ved=2ahUKEwjV4vTR9O2QAxWBEVkFHaSVAMYQre8FegQIBRAt

Hakken, D. (2003). *The Knowledge Landscapes of Cyberspace*. Routledge. https://doi.org/10.4324/9780203505380

Hall, R. H. (1968). Professionalization and Bureaucratization. *American Sociological Review*, *33*(1), 92–104. JSTOR. https://doi.org/10.2307/2092242

Haney, J. M., & Lutters, W. (2018). "It's scary...it's confusing...it's dull": How cybersecurity advocates overcome negative perceptions of security. *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, 411–425. https://dl.acm.org/doi/abs/10.5555/3291228.3291261

Haney, J. M., & Lutters, W. (2019). Motivating Cybersecurity Advocates: Implications for Recruitment and Retention. *Proceedings of the 2019 on Computers and People Research Conference*, 109–117. https://dl-acm-org.proxy-um.researchport.umd.edu/doi/abs/10.1145/3322385.3322388

Haney, J. M., & Lutters, W. G. (2021). Cybersecurity advocates: Discovering the characteristics and skills of an emergent role. *Information & Computer Security*, *29*(3), 485–499. https://doi.org/10.1108/ICS-08-2020-0131

Harry, C. (2015). *A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact* [Working Paper]. Center for International & Security Studies at Maryland. https://spp.umd.edu/sites/default/files/2019-07/CategorizingDisruptiveCyberActivity%20-%20080615.pdf

Harry, C. (2018). A proposed hierarchical taxonomy for assessing the primary effects of cyber events: A sector analysis 2014-2016. In A. Jøsang (Ed.), *ECCWS 2018 17th European Conference on Cyber Warfare and Security* (Vol. 2, pp. 199–207). https://doi.org/10.13016/M26M33675

Harry, C. (2020, February 27). *Integrative paper advisory meeting* [Personal communication].

Harry, C., & Gallagher, N. (2019). *An Effects Centric Approach to Assessing Cyber Risk*. University of Maryland. https://cissm.umd.edu/research-impact/publications/effects-centric-approach-assessing-cybersecurity-risk

Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy*, *5*(2), 302–325. https://doi.org/10.1080/23738871.2020.1792956

Hillmer, U. (2009). Existing Theories Considering Technology Adoption. In U. Hillmer (Ed.), *Technology Acceptance in Mechatronics: The Influence of Identity on Technology Acceptance* (pp. 9–28). Gabler. https://doi.org/10.1007/978-3-8349-8375-6_3

Hong, M., Steedle, J. T., & Cheng, Y. (2020). Methods of Detecting Insufficient Effort Responding: Comparisons and Practical Recommendations. *Educational and Psychological Measurement*, *80*(2), 312–345. https://doi.org/10.1177/0013164419865316

Honeycutt, H. (2019, September 30). *Nature and Nurture as an Enduring Tension in the History of Psychology*. Oxford Research Encyclopedia of Psychology. https://doi.org/10.1093/acrefore/9780190236557.013.518

Hubbard, D. W. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It.* John Wiley & Sons.https://www.google.com/books/edition/_/u2AceU1L95EC?hl=en&sa=X&ved=2ahUKEwi8zJrl9e2QAxVBFlkFHRxUIGkQre8FegQIBRAf

Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk*. John Wiley & Sons. https://www.google.com/books/edition/_/AwD0BgAAQBAJ?hl=en&sa=X&ved=2ahUKEwj5oZKJ9u2QAxV9LFkFHT57CFEQre8FegQIBRAT

Ionita, D. (2013). *Current established risk assessment methodologies and tools* [Thesis, University of Twente]. https://essay.utwente.nl/63830/

ISACA. (2025). *State of Cybersecurity 2025*. ISCAC. https://www.isaca.org/resources/reports/state-of-cybersecurity-2025

(ISC)^2. (2023). *(ISC)2 Cybersecurity Workforce Study 2023*. (ISC)2. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4

(ISC)^2. (2025, July 16). *ISC2 Survey: 30% of Cyber Pros Using AI Security Tools*. https://www.isc2.org/Insights/2025/07/2025-isc2-ai-pulse-survey

JohnPaul, A. C., & Nwalozie, G. (2024). Investigating And Addressing Security Policy Misconfigurations. *IOSR Journal of Engineering*, *14*(4), 1–12. https://www.iosrjen.org/Papers/vol14_issue4/2/A1404020112.pdf

Johnston, A., Gangi, P. D., Howard, J., & Worrell, J. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. *Journal of the Association for Information Systems*, *20*(3). https://doi.org/10.17705/1jais.00533

Kaye, J., Muro, M., & Megas, K. (2021, October 20). *Protecting critical infrastructure from a cyber pandemic*. World Economic Forum. https://www.weforum.org/agenda/2021/10/protecting-critical-infrastructure-from-cyber-pandemic/

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, *38*(2), 7–40. https://doi.org/10.1162/ISEC_a_00138

Khalili, M. M., Liu, M., & Romanosky, S. (2019). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz010

Knott, J. H. (1993). Comparing Public And Private Management: Cooperative Effort And Principal-Agent Relationships. *Journal of Public Administration Research and Theory*, *3*(1), 93–119. https://doi.org/10.1093/oxfordjournals.jpart.a037164

Kurii, Y., & Opirskyy, I. (2022, October 13). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2022)*. International Conference on Problems of Infocommunications. Science and Technology (PICST 2022), Kyiv, Ukraine. https://ceur-ws.org/Vol-3288/paper3.pdf

Kush, J. (2025). *The Human-Machine Identity Blur: A Unified Framework for Cybersecurity Risk Management in 2025*. arXiv. https://arxiv.org/pdf/2503.18255?

Lai, P. C. (2017). The Literature Review of Technology Adoption Models and Theories for the Novelty Technology. *Journal of Information Systems and Technology Management*, *14*(1), 21–38. https://papers.ssrn.com/abstract=3005897

Landoll, D. (2011). *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments* (2nd ed.). CRC Press. https://www.crcpress.com/The-Security-Risk-Assessment-Handbook-A-Complete-Guide-for-Performing/Landoll/p/book/9781439821480

Lawson, S., & Middleton, M. K. (2019). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. *First Monday*. https://doi.org/10.5210/fm.v24i3.9623

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Lee, R. M., Conway, T., & Parsons, D. (2024, September 3). *The Business Risks of Ignoring ICS Security* [Technical Presentation]. https://www.sans.org/webcasts/business-risks-ignoring-ics-security

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Industry 4.0 and national security: The phenomenon of disruptive technology. *Entrepreneurship and Sustainability Issues*, *6*(3), 1528–1535. https://doi.org/10.9770/jesi.2019.6.3(33)

Lipner, S. B., & Lampson, B. W. (2016). *Risk Management and the Cybersecurity of the U.S. Government: Input to the Commission on Enhancing National Cybersecurity*. https://www.nist.gov/system/files/documents/2016/09/16/s.lipner-b.lampson_rfi_response.pdf

Lipsky, M. (2010). Street-Level Bureaucracy, 30th Anniversary Edition: Dilemmas of the Individual in Public Service. Russell Sage Foundation. https://www.google.com/books/edition/Street_Level_Bureaucracy_30th_Anniversar/cs_djgS5v-UC?hl=en&gbpv=0

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

March, J. G., & Olsen, J. P. (2008). The Logic of Appropriateness. In R. Goodin, Michael Moran, & M. Rein (Eds.), *The Oxford Handbook of Public Policy*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199548453.003.0034

Mehta, A. (2020, March 20). *Pentagon declares defense contractors 'critical infrastructure,' must continue work*. Defense News. https://www.defensenews.com/pentagon/2020/03/20/pentagon-declares-defense-contractors-critical-infrastructure-must-continue-work/

Meier, K. J., & Bohte, J. (2000). Ode to Luther Gulick: Span of Control and Organizational Performance. *Administration & Society*, *32*(2), 115–137. https://doi.org/10.1177%2F00953990022019371

Mills, S., & Goldsmith, R. (2014). *Cybersecurity Challenges for Program Managers* (No. ADA610756). Defense Acquisition University. https://apps.dtic.mil/sti/citations/ADA610756

Moallem, A. (2021). Understanding Cybersecurity Technologies: A Guide to Selecting the Right Cybersecurity Tools (1st edition). CRC Press. https://www.google.com/books/edition/Understanding_Cybersecurity_Technologies/sO5LEAAAQBAJ?hl=en&gbpv=0

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Moteff, J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences (CRS Report for Congress No. RL32561). Congressional Research Service. https://fas.org/sgp/crs/homesec/RL32561.pdf

Mun, J., & Housel, T. (2023). Artificial Intelligence and Machine Learning Applications to Navy Ships: Cybersecurity and Risk Management. *Naval Engineers Journal*, *135*(1), 1–23. https://www.ingentaconnect.com/contentone/asne/nej/2023/00000135/00000001/art00018

NACD. (2023). *Director's Handbook on Cyber-Risk Oversight*. National Association of Corporate Directors. https://www.nacdonline.org/globalassets/public-pdfs/nacd_cyber-risk-oversight-handbook_pages_web-compressed.pdf

National Conference of State Legislatures. (2021, August 24). Revolving Door Prohibitions. *Revolving Door Prohibitions*. https://www.ncsl.org/research/ethics/50-state-table-revolving-door-prohibitions.aspx

National Institute of Standards and Technology. (2014). *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST Special Publication (SP) 800-37 Rev. 1 (Withdrawn)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r1

National Institute of Standards and Technology Joint Task Force. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication (SP) 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

National Science and Technology Council. (2016). *2016 Federal Cybersecurity Research and Development Strategic Plan*. National Science and Technology Council. https://catalog.data.gov/dataset/2016-federal-cybersecurity-research-and-development-strategic-plan

Nicholson, D. (2018). Cloud first – tackling the security challenges. *Computer Fraud & Security*, *2018*(1), 8–11. https://doi.org/10.1016/S1361-3723(18)30005-8

Norris, D. (2025). *Cybersecurity for Local Governments*. https://cybersecurity.umbc.edu/cybersecurity-for-local-governments/

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review*, *79*(6), 895–904. https://doi.org/10.1111/puar.13028

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, *43*(8), 1173–1195. https://doi.org/10.1080/07352166.2020.1727295

Norris, D. F., & Reddick, C. G. (2013). Local E-Government in the United States: Transformation or Incremental Change? *Public Administration Review*, *73*(1), 165–175. https://doi.org/10.1111/j.1540-6210.2012.02647.x

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 60–68. https://doi.org/10.1109/STAST.2011.6059257

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & Management*, *58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507

Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? *International Journal of Project Management*, *34*(8), 1568–1578. https://doi.org/10.1016/j.ijproman.2016.08.002

Ostrom, E. (2007). Institutional Rational Choice: An Assessment of the Institutional Analysis and Development Framework. In P. A. Sabatier (Ed.), *Theories of the Policy Process* (2nd ed., pp. 21–64). Westview Press. https://www.taylorfrancis.com/chapters/edit/10.4324/9780367274689-2/institutional-rational-choice-elinor-ostrom

Pala, A., & Zhuang, J. (2019). Information Sharing in Cybersecurity: A Review. *Decision Analysis*, *16*(3), 172–196. https://doi.org/10.1287/deca.2018.0387

Panagiotis, T., Robinson, N., Hellgren, T., Cox, K., Retter, L., & Burnett, P. (2013). *National-level Risk Assessments: An Analysis Report—ENISA*. ENISA. https://www.enisa.europa.eu/publications/nlra-analysis-report

Parsons. (2018). *Industrial Control Systems Cybersecurity: Survey of Engineering and Operational Technology Professionals* [Critical Infrastructure Risk Assessment]. Parsons. http://www.parsons.com/wp-content/uploads/2018/08/Parsons_2018_Critical_Infrastructure_Risk_Assessment.pdf

Pettigrew, K. E. (1999). Waiting for chiropody: Contextual results from an ethnographic study of the information behaviour among attendees at community clinics. *Information Processing & Management*, *35*(6), 801–817. https://doi.org/10.1016/S0306-4573(99)00027-8

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pienta, D., Thatcher, J., Wright, R., & Roth, P. (2024). An Empirical Investigation of The Unintended Consequences of Vulnerability Assessments Leading to Betrayal. *Journal of the Association for Information Systems*, *25*(4), 1079–1116. https://doi.org/10.17705/1jais.00875

Polit, D. F., & Beck, C. T. (2010). Generalization in quantitative and qualitative research: Myths and strategies. *International Journal of Nursing Studies*, *47*(11), 1451–1458. https://doi.org/10.1016/j.ijnurstu.2010.06.004

Powell, W. (2025). *The CISO 3.0: A Guide to Next-Generation Cybersecurity Leadership*. CRC Press. https://www.google.com/books/edition/The_CISO_3_0/opZjEQAAQBAJ?hl=en&gbpv=0

Prall, D. (2017, May 30). The weakest link in your cybersecurity chain. *American City and County*. https://www.americancityandcounty.com/2017/05/30/the-weakest-link-in-your-cybersecurity-chain/

PwC. (2025, January 27). *IAASB Approved Standard: International Standard on Sustainability Assurance (ISSA) 5000, General Requirements for Sustainability Assurance Engagements*. https://viewpoint.pwc.com/dt/gx/en/pwc/auditing_in_briefs/ext/external-users/iaasb-approved-standard.html

Ramezan, C. A. (2025). Understanding the chief information security officer: Qualifications and responsibilities for cybersecurity leadership. *Computers & Security*, *152*, 104363. https://doi.org/10.1016/j.cose.2025.104363

Ramirez, A., Aiello, A., & Lincke, S. J. (2020). A Survey and Comparison of Secure Software Development Standards. *2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275)*, 1–6. https://doi.org/10.1109/CMI51275.2020.9322704

Randall, R. G., & Allen, S. (2021). Cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry. *International Journal of Critical Infrastructure Protection*, *34*, 100454. https://doi.org/10.1016/j.ijcip.2021.100454

Ratcliffe, C. (2020, September 24). Beginner's Guide to Cyber Risk Quantification for CISOs & Cyber Pros in any Sized Business. *Boardish*. https://www.boardish.io/beginners-guide-to-cyber-risk-quantification-for-cisos-cyber-pros/

Reddick, C. G. (2009). Homeland Security Preparedness and Information Systems: Strategies for Managing Public Policy. IGI Global. https://www.google.com/books/edition/Homeland_Security_Preparedness_and_Infor/NaT_Fob6lBIC?hl=en&gbpv=0

Redlein, A., Baretschneider, C., & Thrainer, L. (2025). ESG monitoring and optimisation solutions and their return on investment: Results of several case studies. *IOP Conference Series: Earth and Enironmental Science*. https://www.researchgate.net/publication/370612580_ESG_monitoring_and_optimisation_solutions_and_their_return_on_investment_results_of_several_case_studies

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk Management. In A. Refsdal, B. Solhaug, & K. Stølen (Eds.), *Cyber-Risk Management* (pp. 33–47). Springer International Publishing. https://doi.org/10.1007/978-3-319-23570-7_5

Roberto, M., Bohmer, R. M. J., & Edmondson, A. C. (2006, November 1). Facing Ambiguous Threats. *Harvard Business Review*, *November 2006*. https://hbr.org/2006/11/facing-ambiguous-threats

Rogers, E. M. (2003). *Diffusion of Innovations, 5th Edition* (5th edition). Free Press. https://www.google.com/books/edition/Diffusion_of_Innovations_5th_Edition/9U1K5LjUOwEC?hl=en&gbpv=0

Rosacker, K. M., & Olson, D. L. (2008). Public sector information system critical success factors. *Transforming Government: People, Process and Policy*, *2*(1), 60–70. https://doi.org/10.1108/17506160810862955

Sambamurthy, V., & Subramani, M. (2005). Special Issue on Information Technologies and Knowledge Management. *MIS Quarterly*, *29*(1), 1–7. JSTOR. https://doi.org/10.2307/25148665

Sbriz, L. (2024, November 18). Adding Value with Risk Based Information Security. *ISACA Now Blog*. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/adding-value-with-risk-based-information-security

Scott, J. (2000). Rational Choice Theory. In G. Browning, A. Halcli, & F. Webster (Eds.), *Understanding Contemporary Society: Theories of the Present* (pp. 126–138). Sage Publications. https://www.google.com/books/edition/Understanding_Contemporary_Society/r5N7r69X7L4C?hl=en&gbpv=0

ScienceDirect. (2025). *Association Rules—An Overview*. https://www.sciencedirect.com/topics/computer-science/association-rules

Setiawan, A., Mufti, A., Mau, F. A., Purkoni, A., & Setiawan, A. (2025). Bridging Cybersecurity and Enterprise Risk Management in the Digital Era. *TechComp Innovations: Journal of Computer Science and Technology*, *2*(1), 28–38. https://doi.org/10.70063/techcompinnovations.v2i1.66

Shier, J. (2021, August 30). *What IT security teams can learn from the Colonial Pipeline ransomware attack*. ITProPortal. https://www.itproportal.com/features/what-it-security-teams-can-learn-from-the-colonial-pipeline-ransomware-attack/

Simon, H. A. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, *69*(1), 99–118. https://doi.org/10.2307/1884852

Slayton, R. (2020). Performing Cybersecurity Expertise: Challenges for Public Utility Commissions. *Berkeley Technology Law Journal*, *35*(3), 757–792. https://doi.org/10.15779/Z380R9M47Q

Slayton, R., & Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation & Governance*, *12*(1), 115–130. https://doi.org/10.1111/rego.12168

Smith, D., & Fischbacher, M. (2009). The changing nature of risk and risk management: The challenge of borders, uncertainty and resilience. *Risk Management*, *11*, 1–12. https://doi.org/10.1057/rm.2009.1

Star, S. L., & Griesemer, J. R. (1989). Institutional Ecology, `Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social Studies of Science*, *19*(3), 387–420. https://doi.org/10.1177/030631289019003001

Steele, K., & Stefánsson, H. O. (2020). Decision Theory. In *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/win2020/entries/decision-theory/

Straub, E. T. (2009). Understanding Technology Adoption: Theory and Future Directions for Informal Learning. *Review of Educational Research*, *79*(2), 625–649. https://doi.org/10.3102/0034654308325896

Summers, R. (2022, January 20). The Pentagon's Revolving Door Keeps Spinning: 2021 in Review. *Project On Government Oversight*. https://www.pogo.org/analysis/2022/01/the-pentagons-revolving-door-keeps-spinning-2021-in-review

Tan, P.-N., Steinbach, M., Karpatne, A., & Kumar, V. (2018). *Introduction to Data Mining* (2nd ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/Tan-Introduction-to-Data-Mining-2nd-Edition/P200000003204

Tarhini, A., Arachchilage, N. A. G., Masa'deh, R., & Abbasi, M. S. (2015). A Critical Review of Theories and Models of Technology Adoption and Acceptance in Information System Research. *International Journal of Technology Diffusion (IJTD)*, *6*(4), 58–77. https://doi.org/10.4018/IJTD.2015100104

The Open Group. (2009). *Technical Standard: Risk Taxonomy*. The Open Group. https://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

Thompson, V. A. (1965). Bureaucracy and Innovation. *Administrative Science Quarterly*, *10*(1), 1–20. https://doi.org/10.2307/2391646

Tisdale, S. M. (2016). Architecting a Cybersecurity Management Framework: Navigating and Traversing Complexity, Ambiguity, and Agility [D.Sc., Robert Morris University]. In *ProQuest Dissertations and Theses*. https://www.proquest.com/docview/2051879908/abstract/EF651A72ACA44F88PQ/1

Turner, T. (2025). *SEC547: Defending Product Supply Chains* [Technical Presentation]. https://www.sans.org/cyber-security-courses/defending-product-supply-chains

Turton, W., & Mehrota, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

E-Government Act of 2002, Public Law 107—347, Pub. L. No. 107–347, 116 STAT 2899 2946 (2002). https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

U.S.A. v. Fathi (16 CR 48). (2016). https://www.justice.gov/opa/file/834996/download

US Congress (2022). Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117–03, H.R.2471 (2022). https://www.congress.gov/bill/117th-congress/house-bill/2471

US Cybersecurity and Infrastructure Security Agency (CISA). (2022). *2021 Trends Show Increased Globalized Threat of Ransomware* (Alert (AA22-040a)). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

US Department of Homeland Security Science and Technology Directorate (DHS S&T). (2018). *Cyber Risk Economics Capability Gaps Research Strategy* (p. 44). https://www.dhs.gov/sites/default/files/publications/3950_CYRIE_Report_FINAL508.pdf

US Federal Bureau of Investigations. (2021). *Indicators of Compromise Associated with Cuba Ransomware*. US Federal Bureau of Investigation Cyber Division. https://www.ic3.gov/Media/News/2021/211203-2.pdf

US Federal Bureau of Investigations. (2025). *2024 Annual Internet Crime Report*. Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

US Government Accountability Office. (2008). *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (GAO-08-588). https://www.gao.gov/products/GAO-08-588

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

Verizon. (2022). *2021 Data Breach Investigations Report*. Verizon. https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon. https://www.verizon.com/business/resources/reports/dbir/

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? | Emerald Insight. *Information & Computer Security*, *26*(1). https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2017-0025/full/html

Ward, M. A., & Mitchell, S. (2004). A comparison of the strategic priorities of public and private sector information resource management executives. *Government Information Quarterly*, *21*(3), 284–304. https://doi.org/10.1016/j.giq.2004.04.003

White House. (2013). *Presidential Policy Directive -21: Critical Infrastructure Security and Resilience*. White House Office of the Press Secretary. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

White House. (2018). *National Cyber Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security* (6th ed.). Cengage. /c/management-of-information-security-6e-whitman/9781337405713PF

Williams, D. J., & Noyes, J. M. (2007). How does our perception of risk influence decision-making? Implications for the design of risk information. *Theoretical Issues in Ergonomics Science*, *8*(1), 1–35. https://doi.org/10.1080/14639220500484419

Yanyan, Z., & Yuan, Y. (2010). Study of database intrusion detection based on improved association rule algorithm. *2010 3rd International Conference on Computer Science and Information Technology*, *4*, 673–676. https://doi.org/10.1109/ICCSIT.2010.5565031

Zhou, P., Chen, M., Chang, K.-W., & Zaniolo, C. (2018). Quantification and Analysis of Scientific Language Variation Across Research Fields. *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, 199–203. https://doi.org/10.1109/ICDMW.2018.00037