Carnegie Mellon University
HeinzCollege
INFORMATION SYSTEMS • PUBLIC POLICY • MANAGEMENT

Heinz College of
Information Systems and Public Policy
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, Pennsylvania 15213-3890

June 23rd, 2023

Office of the Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-1090

Re: File No. S7-09-22
Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Office of the Secretary:

This letter is being submitted to request your consideration of the attached thesis, titled "Boardrooms and Breaches: Defining Cybersecurity Expertise for Corporate Directors", which specifically focuses on the "Cybersecurity Expertise" element of the "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies". Within this thesis, we have conducted a comparative analysis between the SEC guidelines for "Cybersecurity Expertise" and the fundamental considerations for "Audit Committee Financial Expert", a similar expert designation. We have synthesized several key observations and recommendations and identified various attributes and professional credentials for cybersecurity governance, risk, and compliance that boards may want to consider when selecting cyber experts. We hope that our research efforts will empower effective decision-making by regulators and organizations alike regarding cyber governance at the board level.

Please do not hesitate to contact us with any questions, comments, or concerns. We are happy to discuss this matter further.

Respectfully yours,

Matthew Nicolai

M.S. in Information Security Policy and Management
Carnegie Mellon University
mnicolai@alumni.cmu.edu

Boardrooms and Breaches: Defining Cybersecurity Expertise for Corporate Directors

Matthew Edward Nicolai
B.A. in Political Science, University of California, Riverside

Submitted in partial fulfillment of the requirements for
the degree of
Master of Science
in
Information Security Policy and Management
Heinz College of Information Systems and Public Policy

Carnegie Mellon University
May 2023

Acknowledgments:

Thank you very much to my thesis advisor, Matthew Butkovic, for your patient guidance throughout this academic endeavor. I am also extremely appreciative of my family for their endless love and support. Thank you to my dear ISPM friends and girlfriend, Olivia, for always being there for me throughout this journey. Thank you to Tim Morrow, Situational Awareness, and the rest of my colleagues at CERT for constantly encouraging my professional development. Finally, thank you to Randy Trzeciak and the rest of the Heinz College team for facilitating my graduate education. Pursuing my graduate degree at Carnegie Mellon has been a challenging and rewarding opportunity that I will cherish forever.

Table of Contents

List of Tables:

Abstract:

This thesis seeks to identify a set of criteria that can serve as a functional definition for the term "cybersecurity expertise" within the context of the U.S. Securities and Exchange Commission (SEC) proposed regulations regarding board-level cybersecurity expertise disclosure. We hope to develop a better understanding of the necessary qualifications for board-level cyber risk oversight and governance by conducting a comparative analysis of the SEC's proposed guidelines against the SEC's longstanding definition of a similar expert role, the Audit Committee Financial Expert. We will present observations and recommendations in a manner that aligns with the fundamental considerations underpinning the SEC's definition of Audit Committee Financial Expert. Furthermore, we will identify various attributes and professional credentials for cybersecurity governance, risk, and compliance that boards may want to consider when selecting cyber experts. Finally, we will discuss areas of future research within this domain.

Chapter 1: Introduction

1.1 - Introduction

On March 9th, 2022, the U.S. Securities and Exchange Commission (SEC) proposed several regulatory changes that may require corporate boards of directors to take a more definitive role in cybersecurity governance. If the revised regulations are approved, corporate boards will be required to disclose their cybersecurity expertise to shareholders, among other information.[1] Boards that lack cybersecurity expertise will likely need to find a way to develop and demonstrate competence to shareholders to avoid potential negative market pressure, such as reduced market value. The SEC hopes these regulations will encourage companies to recruit directors with substantial cybersecurity experience. However, the SEC's open-ended definition of cybersecurity expertise has created significant uncertainty regarding the necessary qualifications.

1.2 - Motivation:

Recent research efforts by organizations such as Forbes, the CAP Group, FactSet, and the Wall Street Journal have sought to evaluate the average level of corporate board readiness regarding the proposed regulatory changes. However, these studies have primarily relied upon "executive-level experience [in the field of cybersecurity] as being indicative of expertise," which may be an insufficient standard due to the broad and complex nature of cybersecurity.[2] Furthermore, these board readiness surveys have utilized different research methodologies,

[1] "SEC.Gov | SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," accessed April 15, 2023, https://www.sec.gov/news/press-release/2022-39.
[2] Rob Sloan, "Analyzing Board-Level Cybersecurity Experience," WSJ, accessed April 3, 2023, https://www.wsj.com/articles/analyzing-board-level-cybersecurity-experience-11669674866.

yielding radically different outcomes. For example, Forbes and the CAP Group stated that "90% of boards are not ready for SEC cyber regulations" after using a data analysis process to evaluate the "board-level expertise" of Russel 3000 companies.[3] Meanwhile, a Wall Street Journal and National Association of Corporate Directors (NACD) study found that over 75% of organizations surveyed already had "at least one cyber expert among the directors."[4] While these surveys generally agreed that further progress needs to be made toward promoting cybersecurity expertise at the board level, there is still considerable ambiguity regarding the overall state of readiness within the private sector. The lack of a unified definition for cybersecurity expertise ultimately hinders study design, possibly leading to the underestimation or overestimation of adverse outcomes in response to regulatory change. Furthermore, if minimum benchmarks for cybersecurity expertise are not established, companies may face increased cyber risks from a lack of competency at the executive/governance level, which may hurt investors, customers, and other stakeholders.

1.3 – Formal Problem Statement and Thesis Significance:

Considering the recently proposed SEC regulations, many organizations have conducted research to determine the readiness of corporate boards of directors to disclose their level of cybersecurity expertise. The highly varied results of these surveys, combined with general uncertainty about the definition of cybersecurity expertise, have inspired the conceptual basis of this thesis. We aim to investigate how professional designations, industry certifications, and

[3] Brian Walker, "Council Post: 90% Of Boards Are Not Ready For SEC Cyber Regulations," Forbes, accessed April 2, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/02/06/90-of-boards-are-not-ready-for-sec-cyber-regulations/.
[4] Rob Sloan, "Survey Finds Boards Have Work To Do on Cybersecurity: Executive Summary," WSJ, accessed April 8, 2023, https://www.wsj.com/articles/survey-finds-boards-have-work-to-do-on-cybersecurity-executive-summary-6cf47acb.

other factors may help inform the definition of cybersecurity expertise in the context of SEC regulations.

Identifying the basic qualifications for cybersecurity expertise will provide investors, directors, researchers, and other stakeholders with a better understanding of the SEC's intended outcome for the proposed regulations. Heightened awareness regarding basic qualifications may assist boards with ensuring cybersecurity competency when selecting directors. The proposed course of action aligns with conventional logic, regulatory precedence, and longstanding norms in corporate governance. We hope our comparative analysis will allow organizations to better understand the definition of cybersecurity expertise and make effective decisions regarding cybersecurity governance at the board level.

Chapter 2: Background

2.1 – Background on the SEC

The U.S. Securities and Exchange Commission is an independent federal agency established in the United States pursuant to the Securities Exchange Act of 1934. This agency is led by a commission of five members, who are presidentially appointed and confirmed by the U.S. Senate. The SEC is empowered to carry out numerous responsibilities as dictated by federal law. These tasks include promoting investor education and communication, overseeing trade within U.S. equity and fixed-income markets, reviewing financial statements and disclosures made by publicly traded companies, regulating the investment activities of registered entities (such as mutual funds and investment advisors), evaluating the activities of security exchanges, boards, and subordinate agencies, and promoting transparency by publishing relevant information on the SEC's website.[5] Overall, the SEC plays a significant role in shaping the rules and boundaries of the market and governing the fundamental business practices that underpin most publicly traded companies.

2.2 – The SEC Rulemaking Process

As a regulatory agency, the SEC translates federal laws into actionable requirements for companies to follow.[6] The SEC enumerates and codifies its regulations as part of the Code of Federal Regulations, commonly abbreviated as CFR. The SEC's regulations fall under Title 17,

[5] "SEC.Gov | About the SEC," accessed April 4, 2023, https://www.sec.gov/strategic-plan/about.
[6] "The Laws That Govern the Securities Industry | Investor.Gov," accessed April 4, 2023, https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#sox2002.

Chapter II of the CFR, which is subdivided into numerous Parts, many of which were created in response to federal laws.[7]

SEC regulations have significantly expanded and evolved over time in response to dynamic market conditions. The SEC utilizes a formal rulemaking process to develop their regulations, which can be initiated in several different ways. The first approach is triggered in response to newly created laws, which are passed by Congress and approved by the President. The SEC can also update regulations periodically if allowed by existing laws. Finally, the SEC can establish new rules if they fall within the organization's legal purview. Over the years, a complex latticework of federal laws has provided significant rulemaking authority to the SEC within various financial domains. This broad discretion has allowed the SEC to develop regulations in a relatively expeditious manner compared to legislative rulemaking or judicial process. During the rulemaking process, the SEC will propose new rules or amendments by publishing a rule proposal (which directly outlines the new developments) or releasing an initial "concept release," which introduces a particular topic and potential regulatory responses. Once released, these documents are opened to a period of public commentary. The SEC will review public comments, make any potential changes, and draft a final rule before voting.[8]

2.3 – Legal Foundations of IT Regulation

Laws such as the Securities Act of 1933, Securities Exchange Act of 1934, Sarbanes-Oxley Act, and Dodd-Frank Act have established and bolstered the SEC's ability to regulate

[7] "17 CFR Chapter II -- Securities and Exchange Commission," accessed April 4, 2023, https://www.ecfr.gov/current/title-17/chapter-II.
[8] "SEC.Gov | Investor Bulletin: An Introduction to The U.S. Securities and Exchange Commission – Rulemaking and Laws," accessed April 4, 2023, https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_rulemaking.

publicly traded companies. The SEC generally uses these powers to protect investors from corporate impropriety.[9] For example, Section 404 of the Sarbanes-Oxley Act (SOX) requires companies to "assess the effectiveness of [their] internal controls and report this assessment annually to the SEC." These assessments must be independently reviewed and judged by an external auditor. The broad wording of Section 404 has made the audit process extremely comprehensive and logistically daunting. Section 404 does not directly address cybersecurity, but "modern financial reporting systems are heavily dependent on technology and associated controls," which indirectly leads to "the scrutiny of information security controls for SOX compliance." In a similar vein, Section 302 of SOX requires the company's Chief Executive Officer (CEO) and Chief Financial Officer (CFO) to "personally certify that financial reports are accurate and complete" and "assess and report on the effectiveness of internal controls around financial reporting." Fraud or misrepresentation in this regard may lead to severe penalties and individual liability, which places increased pressure on corporate leaders to ensure the effective implementation, assessment, auditing, and reporting of internal controls, including those related to cybersecurity.[10]

2.4 – Current SEC Posture Regarding Cyber Risk

Another notable example of the SEC's jurisdictional authority is their requirement for publicly traded companies to disclose "timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment

[9] "SEC.Gov | Investor Bulletin: An Introduction to The U.S. Securities and Exchange Commission – Rulemaking and Laws."
[10] "An Overview of Sarbanes-Oxley for the Information Security Professional | SANS Institute," accessed April 21, 2023, https://www.sans.org/white-papers/1426/.

decision."[11] Companies typically disclose these risks in annual regulatory filings, if not more frequently.

Over the years, corporate risks have evolved drastically due to global trends and other phenomena. In turn, the SEC has engaged in regulatory rulemaking and related administrative processes to ensure that companies continue to properly disclose risks. Among the significant risks that have emerged in the modern era, cybersecurity has quickly become a high-priority topic of discussion amongst investors, regulators, and corporate executives.[12] In a recent National Association for Corporate Directors (NACD) survey, 34% of corporate boards ranked cybersecurity as a major concern for their organization over the next twelve months.[13] Furthermore, 45% of boards highlighted crisis management preparation as a major concern for their organization.[14] The significant adverse effects of cyberattacks have made investors wary of potential cyber risks at publicly traded companies. In response, the SEC has emphasized that publicly traded companies should include cybersecurity-related disclosures in their mandatory regulatory filings.

Under current regulations, publicly traded companies must disclose cybersecurity-related risks if they are "among the most significant factors that make an investment in the company

[11] "CF Disclosure Guidance: Topic No. 2 - Cybersecurity," accessed April 4, 2023, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm#_ednref2.
[12] "2022 NACD Public Company Board Practices and Oversight Survey," accessed April 8, 2023, https://www.nacdonline.org/insights/publications.cfm.
[13] Ted Sikora, "Director Perspective: Top Priorities of 2023," *The Harvard Law School Forum on Corporate Governance* (blog), February 10, 2023, https://corpgov.law.harvard.edu/2023/02/10/director-perspective-top-priorities-of-2023/.
[14] Rob Sloan, "Survey Results Part One: Board Directors Have Work To Do on Cybersecurity," WSJ, accessed April 3, 2023, https://www.wsj.com/articles/survey-results-part-one-board-directors-have-work-to-do-on-cybersecurity-697223d0.

speculative or risky." More specifically, SEC Regulation S-K Item 503(c) requires risk disclosure statements to "adequately describe the nature of the material risks" and identify how the risk may affect the company.[15] In practice, the company's cyber risk disclosure often includes a discussion of internal business practices that open the company to cyber risk, outsourced activities that carry cyber risk, cybersecurity incidents that have recently impacted the company, information regarding the company's current cybersecurity insurance coverage, and potentially, the discussion of "known or threatened cyber incidents" that may impact the company. The company's regulatory disclosures may also include the discussion of costs and consequences arising from cybersecurity incidents.[16] Below is an excerpt from SolarWinds' 2021 SEC 10-K regulatory filing, which provides readers with an example of cyber risk disclosure. At the time, SolarWinds was the subject of a notable cybersecurity incident, which is referenced in the filing as "The Cyber Incident":

> "Cyberattacks, including the Cyber Incident, and other security incidents have resulted, and in the future may result, in compromises or breaches of our and our customers' systems, the insertion of malicious code, malware, ransomware or other vulnerabilities into our systems and products and in our customers' systems, the exploitation of vulnerabilities in our and our customers' environments, theft or misappropriation of our and our customers' proprietary and confidential information, interference with our and our customers' operations, exposure to legal and other liabilities, higher customer, employee and partner attrition, negative impacts to our sales, renewals and upgrade and reputational harm and other serious negative consequences, any or all of which could materially harm our business.
>
> The Cyber Incident has had and may continue to have an adverse effect on our business, reputation, customer, employee and partner relations, results of operations, financial condition or cash flows.
>
> As a result of the Cyber Incident, we are party to several lawsuits and are the subject of an ongoing investigation by the SEC, any of which could result in significant costs and expenses, the diversion of management's attention, a negative impact on employee

[15] "CF Disclosure Guidance: Topic No. 2 - Cybersecurity."
[16] "CF Disclosure Guidance: Topic No. 2 - Cybersecurity."

> morale and an adverse effect on our business, reputation, financial condition, results of operations or stock price."[17]

2.5 – Proposed Regulatory Changes

As the cybersecurity threat landscape continues to evolve, the SEC has responded with more aggressive regulations that aim to protect investors from increased cyber risk. The SEC has paid particular attention to emphasizing corporate governance in the context of cybersecurity oversight. Proper governance, especially at the board level, is widely perceived as an essential factor for enabling effective cybersecurity risk management, incident response, and disaster preparation throughout the organization.[18] The SEC has recently proposed several rule changes that will expand the level of mandatory disclosure regarding cyber risk. Under the proposed rules, companies will need to provide details regarding "material" cybersecurity incidents to the SEC within four days of incident discovery. As a point of comparison, Table 1 provides an overview of other major federal data breach laws and regulations and their requirements:

[17] "FORM 10-K SolarWinds Corporation," accessed April 25, 2023, https://www.sec.gov/Archives/edgar/data/1739942/000173994222000020/swi-20211231.htm.
[18] Hetal Kanji, Orla Cox, and Simon Onyons, "Building Effective Cybersecurity Governance," *The Harvard Law School Forum on Corporate Governance* (blog), November 10, 2022, https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/.

Table 1 - Federal Data Breach Reporting Overview

Table 1 - Federal Data Breach Reporting Overview		
Law/Regulation:	**Regulatory Reporting Timeline:**	**Definition of Incident:**
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	• If 500 or more individuals are affected, HHS must be notified no later than 60 days post-breach[19] • If less than 500 individuals are affected, can be reported to HHS on an annual basis[20]	"The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[21]
Defense Federal Acquisition Regulation Supplement (DFARS)	Within 72 hours of the incident[22]	"Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein."[23]
Cyber Incident Reporting for Critical Infrastructure Act of 2022	Within 72 hours of the incident and within 24 hours of ransomware payment[24]	A "cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States."[25]
Computer-Security Incident Notification rule (FDIC/OCC/Federal Reserve)	No later than 36 hours after the determination of incident[26]	An "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."[27]

[19] Office for Civil Rights (OCR), "Breach Notification Rule," Text, HHS.gov, September 14, 2009, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
[20] Rights (OCR).
[21] Office for Civil Rights (OCR), "What Does the Security Rule Require a Covered Entity to Do to Comply with the Security Incidents Procedures Standard?," Text, HHS.gov, April 8, 2010, https://www.hhs.gov/hipaa/for-professionals/faq/2002/what-does-the-security-rule-require-a-covered-entity-to-do-to-comply/index.html.
[22] "DOD Cybersecurity Incident Reporting 062421 Cleared for Public Release AFRL-2021-2004, 25 Jun 2021_1.Pdf," accessed April 22, 2023, https://www.safcn.af.mil/Portals/64/DOD%20Cybersecurity%20Incident%20Reporting%20062421%20Cleared%20for%20Public%20Release%20%20AFRL-2021-2004%2C%2025%20Jun%202021_1.pdf.
[23] "DOD Cybersecurity Incident Reporting 062421 Cleared for Public Release AFRL-2021-2004, 25 Jun 2021_1.Pdf."
[24] "Cyber Incident Reporting: New Rules, New Timelines | Crowe LLP," accessed April 22, 2023, https://www.crowe.com/cybersecurity-watch/cyber-incident-reporting-new-rules-new-timelines.
[25] "Cyber Incident Reporting."
[26] "Cyber Incident Reporting."
[27] "Cyber Incident Reporting."

The proposed SEC regulations will require companies to disclose information about their cybersecurity governance, risk analysis, and management processes. Furthermore, companies will be required to describe the cybersecurity experience of their board members.[28] Among the proposed rules, the final element regarding the disclosure of cybersecurity expertise is novel and significant. Cybersecurity exists as a relatively new area of specialization on the corporate board, primarily due to the nascency of the field in comparison to traditional business areas, such as finance and accounting. Cybersecurity is an incredibly complex and important element of business operations that executives and existing board members may not fully understand. Mature security programs often involve a wide variety of people, policies, and technologies which must be appropriately managed and continually improved to ensure constant alignment with the dynamic cyber threat landscape. Furthermore, the details and nuances of cyber risk extend far beyond traditional business knowledge, which may negatively impact the cybersecurity risk management posture of the organization if proper expertise is not brought to the table.[29] Without proper expertise or guidance, organizations may fall victim to underestimating cyber risks, especially in comparison to other business risks. It is important to note that information systems often have a broad reach across the enterprise environment, which could allow a cybersecurity incident to negatively impact the entire organization in the absence of adequate security controls.[30]

The SEC's proposed rule change is also notable because it is relatively open-ended. The SEC highlights some potential examples of cybersecurity experience that may be counted

[28] Walker, "Council Post."
[29] Walker.
[30] Antoinette King, "Cybersecurity Risk Is Business Risk," Industrial Cybersecurity Pulse, December 28, 2021, https://www.industrialcybersecuritypulse.com/facilities/cybersecurity-risk-is-business-risk/.

towards the determination of cybersecurity expertise, such as prior work experience in the field, relevant degrees/certifications, and "knowledge, skills, or other background in cybersecurity."[31] However, the proposed regulations do not establish any specific minimum requirements for expertise or punishments for not appointing a cyber expert, instead leaving it up to "shareholders and regulators to judge for themselves whether director expertise is sufficient."[32]

It is believed that the SEC's intended outcome for cybersecurity expertise disclosure is to push companies to appoint at least one qualified individual to serve as a cyber expert on their board, as the company may face negative consequences from market forces if they fail to do so. While organizations could technically choose to rely on executives (such as the CIO or CISO) or external consultants to provide security insights to the board, adding at least one cyber expert to the board is expected to promote cybersecurity literacy and advocacy at the highest level of organizational governance.[33] The proposed regulations are arriving at a critically important time, as demonstrated by a recent MIT and Proofpoint survey in which the United States and Canada were ranked as the "least likely to have at least one board member with cybersecurity experience" among 12 major countries, with 62% of U.S. and Canadian boards having cybersecurity experience as compared to 73% globally.[34] Furthermore, surveys have indicated significant variations in board-level cybersecurity expertise depending on the industry, as evidenced by the alarming statistic that over 33% of energy/utility companies do not have a

[31] "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," accessed April 4, 2023, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[32] Walker, "Council Post."
[33] Julia Muccini, "Cybersecurity Experience Disclosure | SEC Disclosure Requirement," *OCD Tech* (blog), March 21, 2022, https://ocd-tech.com/2022/03/21/sec-proposed-rule-could-add-cybersecurity-to-the-boardroom/.
[34] "Board-of-Directors-Cyber-Attitudes.Pdf," accessed April 22, 2023, https://cams.mit.edu/wp-content/uploads/Board-of-Directors-Cyber-Attitudes.pdf.

cybersecurity expert on their board, which may hurt their cyber risk management posture.[35] These statistics suggest that appointing a cyber expert to the board can help promote a "tone at the top" security culture, which hopefully trickles downwards.

2.6 – Drawing Parallels to the Sarbanes-Oxley Act

Over two decades ago, the U.S. Government passed the Sarbanes-Oxley (SOX) Act of 2002, which put several regulatory changes into motion, including establishing the term "Audit Committee Financial Expert," or ACFE. Under Sarbanes-Oxley, the SEC began to require companies to disclose whether their audit committee includes at least one member with financial expertise, implied within the context of auditing and accounting. As such, the SEC coined the term Audit Committee Financial Expert to enumerate and describe the professional attributes that may allow an individual to qualify as an "expert" in auditing and accounting.[36]

Audit Committee Financial Expert is a unique term because it represents one of the few SEC designations that requires specific expertise and has been widely adopted throughout the private sector. For context, audit committees must maintain compliance with SEC regulations, exchange standards, and potential additional requirements from the Public Company Accounting Oversight Board, or PCOAB. The SEC does not require that organizations include an Audit Committee Financial Expert on their audit committee, but the organization must substantiate their rationale regarding the exclusion if they choose not to appoint an expert.[37] Major stakeholders such as the NYSE and NASDAQ have accepted the SEC's definition of Audit

[35] Sloan, "Survey Results Part One."
[36] "SEC Issues Final Rules on Disclosure of Audit Committee Financial Experts and Codes of Ethics," n.d.
[37] "Audit Committee Requirements," Deloitte United States, accessed April 8, 2023, https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/audit-committee-requirements.html.

Committee Financial Expert and modified their listing standards to ensure alignment with the SEC's terminology.[38] As such, the SEC's definition carries considerable weight across the regulatory landscape. Establishing the definition of Audit Committee Financial Expert was relatively arduous from a rulemaking perspective due to the differences in opinion raised during the public commentary period. However, the final definition of the term has gained widespread acceptance and continues to be used today.[39]

[38] "POSSIBLE REVISIONS TO AUDIT COMMITTEE DISCLOSURES," accessed April 8, 2023, https://www.sec.gov/rules/concept/2015/33-9862.pdf.
[39] "SEC Issues Final Rules on Disclosure of Audit Committee Financial Experts and Codes of Ethics."

Chapter 3: Audit Committee Financial Expert

3.1 - Defining ACFE:

The SEC's final definition of Audit Committee Financial Expert is divided into two parts. First, the regulations describe the necessary attributes, followed by a list of pathways to attain those attributes. Analysis begins with a discussion of the required attributes, as described in Table 2:

Table 2 - Required Attributes for Audit Committee Financial Expert

Table 2: Required Attributes for Audit Committee Financial Expert
An understanding of generally accepted accounting principles and financial statements;
The ability to assess the general application of such principles in connection with the accounting for estimates, accruals and reserves;
Experience preparing, auditing, analyzing or evaluating financial statements that present a breadth and level of complexity of accounting issues that are generally comparable to the breadth and complexity of issues that can reasonably be expected to be raised by the registrant's financial statements, or experience actively supervising one or more persons engaged in such activities;
An understanding of internal controls and procedures for financial reporting; and
An understanding of audit committee functions

3.2 – Discussion of Specific Attributes

The first attribute for ACFE designation requires candidates to possess "an understanding of generally accepted accounting principles and financial statements." Generally Accepted Accounting Principles, commonly known as GAAP, refers to a longstanding accounting standard adopted by the SEC that serves as the foundation for modern corporate accounting practices in the United States. GAAP is essential in standardizing the "classifications, assumptions and procedures used in accounting in industries across the US" and provides "clear, consistent and

comparable information on organizations financials."[40] GAAP is characterized by ten key principles, which are described in Table 3:

Table 3 - The 10 Key Principles of GAAP

Table 3: The 10 Key Principles of GAAP
1. Principle of Regularity: "The accountant has adhered to GAAP rules and regulations as a standard."
2. Principle of Consistency: "Accountants commit to applying the same standards throughout the reporting process, from one period to the next, to ensure financial comparability between periods. Accountants are expected to fully disclose and explain the reasons behind any changed or updated standards in the footnotes to the financial statements."
3. Principle of Sincerity: "The accountant strives to provide an accurate and impartial depiction of a company's financial situation."
4. Principle of Permanence of Methods: "The procedures used in financial reporting should be consistent, allowing a comparison of the company's financial information."
5. Principle of Non-Compensation: "Both negatives and positives should be reported with full transparency and without the expectation of debt compensation."
6. Principle of Prudence: "This refers to emphasizing fact-based financial data representation that is not clouded by speculation."
7. Principle of Continuity: "While valuing assets, it should be assumed the business will continue to operate."
8. Principle of Periodicity: "Entries should be distributed across the appropriate periods of time. For example, revenue should be reported in its relevant accounting period."
9. Principle of Materiality: "Accountants must strive to fully disclose all financial data and accounting information in financial reports."
10. Principle of Utmost Good Faith: "Derived from the Latin phrase *uberrimae fidei* used within the insurance industry. It presupposes that parties remain honest in all transactions."[41]

The second attribute for ACFE is "the ability to assess the general application of such principles in connection with the accounting for estimates, accruals and reserves." Essentially,

[40] "Generally Accepted Accounting Principles (GAAP) Guide Sheet," n.d.
[41] "GAAP: Understanding It and the 10 Key Principles," Investopedia, accessed April 11, 2023, https://www.investopedia.com/terms/g/gaap.asp.

this attribute requires the candidate to be able to assess the application of GAAP principles towards key accounting/financial reporting functions, namely "estimates, accruals and reserves."[42]

The third ACFE attribute is focused on experience. As described in Table 2, the SEC formally requires five attributes for ACFE designation. Four of these attributes require "ability" or "understanding," which we will consider synonymous with "Knowledge, Skills, and Abilities" (KSAs) for this study. However, one notable outlier remains, which specifically requires:

> *"Experience preparing, auditing, analyzing or evaluating financial statements that present a breadth and level of complexity of accounting issues that are generally comparable to the breadth and complexity of issues that can reasonably be expected to be raised by the registrant's financial statements"*
>
> **OR**
>
> *"experience actively supervising one or more persons engaged in such activities"*

This "experience" attribute requires the candidate to have previous audit, accounting, or financial analysis/evaluation experience at the individual contributor or managerial level within a similarly complex environment. Auditors, accountants, and financial analysts (e.g., hedge fund analysts) are some of the professional backgrounds that may qualify under this requirement. This attribute is notable because, in practice, it should significantly limit the number of candidates who may qualify for ACFE status. While it may be possible to obtain the other four ACFE attributes through education, the "experience" attribute will likely disqualify candidates who lack

[42] "SEC Issues Final Rules on Disclosure of Audit Committee Financial Experts and Codes of Ethics."

relevant professional work experience. While this attribute will likely disqualify younger, inexperienced professionals (such as new grads), the SEC clarifies that it should also disqualify senior executives with "little active involvement in financial and accounting matters."[43]

The fourth ACFE attribute involves the "understanding of internal controls and procedures for financial reporting." Internal controls are "policies and procedures implemented by an organization to ensure their financial reports are reliable, operations are efficient, and activities comply with applicable laws and regulations." These controls "can be tested and validated by checking to see if specific process steps (such as approval signatures) were followed."[44] This attribute also requires the candidate to understand the "process for communicating financial information" to internal and external stakeholders, including investors and regulators.[45]

The final ACFE attribute requires "an understanding of audit committee functions." The audit committee is responsible for providing "oversight of the financial reporting process, the audit process, the company's system of internal controls and compliance with laws and regulations." The audit committee performs several essential business activities, highlighting the importance of selecting a candidate familiar with the committee's role and impact within the organization.[46]

---

[43] "SEC Issues Final Rules on Disclosure of Audit Committee Financial Experts and Codes of Ethics."
[44] "Definition of Internal Controls - Gartner Finance Glossary," Gartner, accessed April 11, 2023, https://www.gartner.com/en/finance/glossary/internal-controls.
[45] NetSuite.com, "Why Is Financial Reporting Important?," Oracle NetSuite, June 1, 2022, https://www.netsuite.com/portal/resource/articles/accounting/financial-reporting.shtml.
[46] "Audit Committee Role & Responsibilities," accessed April 11, 2023, https://www.cfainstitute.org/en/advocacy/issues/audit-committee-role-practices.

3.3 – Discussion of Attribute Acquisition Pathways

As mentioned in the previous section, the SEC regulations describe four pathways through which the five ACFE attributes must be acquired. These pathways are specified in Table 4:

Table 4 - Pathways for ACFE Acquisition

Table 4 – ACFE Attributes must be acquired through ONE or MORE of the following:
Education and experience as a principal financial officer, principal accounting officer, controller, public accountant or auditor or experience in one or more positions that involve the performance of similar functions
Experience actively supervising a principal financial officer, principal accounting officer, controller, public accountant, auditor or person performing similar functions
Experience overseeing or assessing the performance of companies or public accountants with respect to the preparation, auditing or evaluation of financial statements
Other relevant experience

It is important to note that candidates only need to qualify through **one or more** of the pathways described in Table 4 but must possess **all five attributes** discussed in Table 2. The first pathway listed in Table 4 requires candidates to possess

> *"Education and experience as a principal financial officer, principal accounting officer, controller, public accountant or auditor"*
>
> **OR**
>
> *"experience in one or more positions that involve the performance of similar functions"*

Much like the "experience" attribute described in Section 3.2, the SEC's verbiage for the first pathway suggests that the **combination of education and experience** *or* **experience alone** may allow an individual to qualify, but that **education alone appears insufficient**. It is also

important to note that two of the three specific pathways align with managerial responsibilities, which may inherently promote recruiting candidates from managerial backgrounds. Qualified individuals will likely have experience related to serving as a "principal financial officer, principal accounting officer, controller, public accountant or auditor" or another similar position, likely acting in a management or oversight capacity.

3.4 – Discussion of Key Takeaways

We can derive several key takeaways from the SEC's definition of Audit Committee Financial Expert. The SEC seems to encourage the recruitment of candidates with significant, real-world experience in audit/accounting, and many of the regulations are particularly inclusive for individuals with managerial experience in related domains. The regulations also encourage selecting candidates familiar with accounting standards and best practices. Furthermore, the regulations seem to encourage using experience as a measure of competency and qualification rather than relying on formal education. However, education is inherently ingrained in some of the pathways, as many audit and public accounting positions require Certified Public Accountant (CPA) licensure, which carries a significant educational requirement.[47] Furthermore, these positions commonly serve as pathways into the managerial roles discussed in Table 4, so some candidates may also hold CPA licensure or relevant education.

[47] AICPA, "Adopting the Comprehensive Definition of Attest: Protecting the Public," accessed April 18, 2023, https://us.aicpa.org/content/dam/aicpa/advocacy/state/downloadabledocuments/what-are-attest-services.pdf.

Chapter 4: Cybersecurity Expertise

4.1 – Discussion of Cybersecurity Expertise

The SEC's proposed regulations regarding disclosing board-level cybersecurity expertise include "non-exhaustive" criteria that the company should consider when determining whether a director has cybersecurity expertise.[48] These elements are relatively straightforward, as outlined in Table 5:

Table 5 - Criteria for Cybersecurity Expertise

Table 5 – Criteria for Cybersecurity Expertise
Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;
Whether the director has obtained a certification or degree in cybersecurity; and
Whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

It is important to note that, unlike the ACFE attributes described in Table 2, a director does not need to satisfy all three qualifications listed in Table 4 to demonstrate cybersecurity expertise. Furthermore, there is no codified relationship between the necessary attributes for expertise and the pathways through which one must achieve those attributes, which differs from the ACFE requirements. As a result, the organization, rather than the SEC, maintains significant discretion in determining the baseline qualifications for cybersecurity expertise. This discretion may yield both positive and negative implications. The flexibility of the proposed regulations

[48] "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

could allow organizations to recruit directors who genuinely understand the cyber risk management needs of the organization but may not have a traditional background. On the other hand, providing too much freedom could lead to selecting directors with improper or inadequate expertise, which could hurt shareholders if insufficient qualifications lead to errors or omissions.

4.2 – Discussion of "prior work experience"

The SEC's first category relates to "prior work experience in cybersecurity." The SEC describes several potentially relevant examples of work experience that the board may want to consider, ranging from Information Security Officer to Business Continuity Planner. These roles may share some commonalities under the banner of cybersecurity, but their day-to-day tasks and exposure to the various facets of cybersecurity may vary significantly, especially if the candidate's experience is spread across different companies. As a result, prior work experience should likely not be utilized as a sole indicator of cybersecurity expertise. It is also important to note that, compared to the pathways described in Table 4, there is little differentiation between individual contributor and managerial experience.

4.3 – Discussion of Education

In the proposed regulations, the SEC recommends that boards consider "whether the director has obtained a certification or degree in cybersecurity" as a potential indicator of expertise. The field of cybersecurity commonly utilizes certifications as a method of demonstrating competence in particular domains. Formal educational programs are also quickly emerging to bridge the cyber skills gap.[49] While education is generally a positive factor in any

[49] Debabrata Deb, "Cyber Security Certification vs Degree: Which Is Best for Your Career?," ITPro, February 15, 2023, https://www.itpro.com/business-strategy/careers-training/370054/cyber-security-certification-vs-degree.

context, the nascency of cybersecurity as a distinct academic discipline may require organizations to consider candidates with degrees in related fields, such as computer science or business. Widely accepted industry certifications like the CISSP and CISA may also qualify under the SEC's proposed guidelines.

4.4 – Discussion of Knowledge, Skills, and Abilities

The final SEC guideline evaluates whether the candidate has "knowledge, skills, or other background in cybersecurity," followed by various examples of cybersecurity concepts and related domains. These topics are quite broad, and candidates may have gained exposure via education or work experience.

Chapter 5: Comparative Analysis of ACFE and Cybersecurity Expertise

5.1 – Rationale and Methodology

This thesis aims to perform a comparative analysis between the SEC's outlined guidelines for cybersecurity expertise and the SEC's long-established definition of Audit Committee Financial Expert. Both concepts directly relate to critical compliance activities that play a significant role in corporate governance and risk management. While cybersecurity and auditing may appear to be unrelated professional disciplines at first glance, there is a strong relationship between internal audit and cybersecurity within the corporate environment, especially regarding security controls.[50] Additionally, cybersecurity expertise and ACFE have been the subjects of considerable scrutiny, ambiguity, and discussion during their rulemaking processes. These collective factors suggest that the definition of Audit Committee Financial Expert may be a strong candidate for comparison against cybersecurity expertise within the context of the SEC's proposed regulations.[51]

5.2 – Practical Approach to Comparison

The requirements for Audit Committee Financial Expert and the proposed guidelines for cybersecurity expertise will be extracted from their respective SEC publications in the latest form. Subsequently, these elements will be mapped into different categories, namely "Education," "Work Experience," and "Knowledge, Skills, and Abilities" (KSAs). For this study, the term "understanding," which is commonly used by the SEC, will be considered synonymous with "Knowledge, Skills, and Abilities" (KSAs), and grouped as such.

[50] "Cybersecurity and Internal Audit," Deloitte United States, accessed April 8, 2023, https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html.
[51] "SEC Issues Final Rules on Disclosure of Audit Committee Financial Experts and Codes of Ethics."

5.3 – Developing Observations and Recommendations

We will perform a comparative analysis between ACFE and cybersecurity expertise within the three categories outlined in Section 5.2. We will utilize our observations to develop recommendations for assessing cybersecurity expertise more granularly. Our recommendations will consider the various factors underpinning ACFE.

5.4 – Comparative Analysis between Cybersecurity Expertise and ACFE

In Table 6, we have created a framework for comparing Cybersecurity Expertise and Audit Committee Financial Expert. We have categorized the guidelines and requirements for each designation under the categories of "Work Experience," "Education," and "Knowledge, Skills, and Abilities":

Table 6 - Comparison of Cybersecurity Expertise and Audit Committee Financial Expert

Table 6 - Comparison of Cybersecurity Expertise and Audit Committee Financial Expert			
Category:	**Cybersecurity Expertise**	**Audit Committee Financial Expert**	**Observations:**
Work Experience	Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security opersations or incident response manager, or business continuity planner;	Experience preparing, auditing, analyzing or evaluating financial statements that present a breadth and level of complexity of accounting issues that are generally comparable to the breadth and complexity of issues that can reasonably be expected to be raised by the registrant's financial statements, or experience actively supervising one or more persons engaged in such activities; Experience actively supervising a principal financial officer, principal accounting officer, controller, public accountant, auditor or person performing similar functions; Experience overseeing or assessing the performance of companies or public accountants with respect to the preparation, auditing or evaluation of financial statements; or Other relevant experience	• The examples of prior work experience for Cybersecurity Expertise are broad in comparison to ACFE • The ACFE requirements include a caveat requiring the "breadth and level of complexity" of experience to be "generally comparable" to ACFE responsibilities • The examples of prior experience for cybersecurity expertise do not differentiate between individual contributor or manager-level experience
Education	Whether the director has obtained a certification or degree in cybersecurity; and	Education *and experience* as a principal financial officer, principal accounting officer, controller, public accountant or auditor *or experience* in one or more positions that involve the performance of similar functions;	• "Cybersecurity expertise" discusses only education, while ACFE mentions education ***and*** experience • Several of the ACFE roles require formal education for licensure (e.g., CPA) • ACFE does not specifically mention degrees or certifications
Knowledge, Skills, and Abilities (KSAs)	Whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.	An understanding of generally accepted accounting principles and financial statements; The ability to assess the general application of such principles in connection with the accounting for estimates, accruals and reserves; An understanding of internal controls and procedures for financial reporting; and An understanding of audit committee functions	• The KSAs for cybersecurity expertise are very broad in comparison to ACFE • Cyber KSAs do not touch upon the understanding and application of standards (e.g., NIST/ISO), unlike ACFE • ACFE requires an understanding of financial reporting and the audit committee; no parallel example for cybersecurity expertise

5.5 – Observations for “Work Experience”

We can observe several key differences in the “Work Experience” category. Initially, we can identify a difference in the granularity of the experience requirements for ACFE and Cybersecurity Expertise. ACFE requires candidates to perform specific tasks within certain finance/accounting domains. Meanwhile, Cybersecurity Expertise makes no such differentiation, instead relying on job titles rather than functional responsibilities.

ACFE also includes a caveat that requires candidates to have experience with accounting issues that are “generally comparable to the breadth and complexity of issues that can reasonably be expected to be raised by the registrant's financial statements.” In this case, the registrant would be the organization where the candidate wants to serve as ACFE. We cannot observe a similar breadth and complexity requirement for cybersecurity expertise.

In the requirements for ACFE, we can also identify terminology relating to the differentiation between individual contributor and managerial responsibilities, as indicated by the terms “supervising,” “overseeing,” and “assessing.” While some of these actions may find parallels within the roles listed for cybersecurity expertise, they are not enumerated. As discussed in previous sections, the clear delineation (and acceptance of) of individual contributor and managerial responsibilities may inherently encourage the selection of candidates with managerial experience, but the terminology is also relatively inclusive.

5.6 – Observations for “Education”

Cybersecurity Expertise only discusses whether a candidate has a degree or certification in cybersecurity, while the ACFE requirements discuss education in conjunction with experience. As such, the ACFE requirements may inherently create a higher “floor” for prerequisite work experience compared to Cybersecurity Expertise. It is also important to note that many of the roles discussed within the context of ACFE either require or highly prefer licensure as a Certified Public Accountant, which generally carries a significant formal education requirement. Explicit discussion of degrees or certifications is not found under ACFE requirements, but they can be implied based on some job responsibilities (e.g., CPA).

5.7 – Observations for “Knowledge, Skills, and Abilities (KSAs)”

Within the Knowledge, Skills, and Abilities (KSAs) category, we can observe a fundamental difference in the requirements for ACFE and the guidelines for Cybersecurity Expertise. More specifically, the ACFE requirements require an understanding of GAAP and the ability to assess the application of these principles. ACFEs are also required to understand internal controls, financial reporting, and the audit committee's function. On the Cybersecurity Expertise side, we can only observe general discussion of KSAs in different cyber domains, ranging from security policy and governance to business continuity planning. There is a stark difference between ACFE and Cybersecurity Expertise regarding the knowledge and application of standards and best practices.

5.8 – Recommendations

In Table 7, found below, we have outlined our observations from Table 6 and developed recommendations to address the corresponding gaps and potential shortcomings. Both publicly traded companies and the SEC can leverage these recommendations to make more informed decisions regarding the fundamental basis of cybersecurity expertise at the board level. The recommendations reconcile differences between ACFE considerations and cybersecurity expertise guidelines, providing insights rooted in regulatory precedence.

Table 7 - Observations and Recommendations

Table 7 - Observations and Recommendations		
Category:	**Observations:**	**Recommendations:**
Work Experience	The examples of prior work experience for Cybersecurity Expertise are broad in comparison to ACFE	When considering the selection of a cyber expert, boards should utilize a more detailed breakdown of acceptable work experience that aligns with the current industry landscape, such as those required for CISSP and CISA certifications
	The ACFE requirements include a caveat requiring the "breadth and level of complexity" of experience to be "generally comparable" to ACFE responsibilities	Boards should consider whether the candidate's past work experience is commensurate with the expected responsibilities of the board cyber expert. Furthermore, the SEC should consider amending the guidelines to encourage the selection of experts with commensurate experience.
	The examples of prior experience for cybersecurity expertise do not differentiate between individual contributor or manager level experience	Boards should consider candidates from diverse backgrounds, including in-house security personnel and external assessors/auditors/consultants, but should also consider whether the candidate has sufficient breadth of expertise to address the governance responsibilities of being a director on the board
Education	"Cybersecurity expertise" discusses only education, while ACFE mentions education ***and*** experience	Boards should ideally consider candidates with a combination of cybersecurity education and work experience; boards may prefer candidates who hold certifications that require verifiable work experience.
	Several of the ACFE roles require formal education for licensure (e.g., CPA)	Cybersecurity is different from many other fields as it does not require licensure or formal education for most roles. Boards may want to consider requiring certifications such as CISSP and CISA in the absence of a licensing authority or formal education requirements.
	ACFE does not specifically mention degrees or certifications	Formal education is required for many of the ACFE prerequisite roles; the SEC may want to incorporate it into future regulations.
Knowledge, Skills, and Abilities (KSAs)	The KSAs for cybersecurity expertise are very broad in comparison to ACFE	Organizations may want to consider referencing a common body of knowledge for cybersecurity, such as the $(ISC)^2$ CBK. The SEC may also want to consider further refining the regulations.
	Cyber KSAs do not touch upon the understanding and application of standards (e.g., NIST/ISO), unlike ACFE	The SEC and corporate boards should require cyber experts to have a working knowledge of cybersecurity standards and best practices, including assessment and implementation.
	ACFE requires an understanding of financial reporting and the audit committee; no parallel example for cybersecurity expertise	The SEC and corporate boards should require cyber experts to have a working understanding of cybersecurity operations, security architecture, and the reporting structure of the organization.

Chapter 6: Comparative Analysis between Professional Credentials

6.1 – Recommendation Methodology

In Chapter 5, we reconciled the fundamental differences between the ACFE requirements and proposed guidelines for Cybersecurity Expertise. We subsequently synthesized our observations to develop recommendations for corporate boards and the SEC to consider. In this section, we will shift our focus toward evaluating professional credentials that may help us define cybersecurity expertise.

In Table 7, we have outlined the work experience, education, and examination requirements for several credentials closely related to cybersecurity governance, risk, and compliance, specifically the Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA). Industry certifications are important in cybersecurity, as they can bridge the gap between formal education and necessary professional skills. Notably, these certifications have an experience and/or education requirement, and many organizations prefer (or sometimes require) candidates to hold these certifications, which creates a "de facto" minimum standard for cybersecurity experience and education in many cases.

We have selected CISSP and CISA for comparison because they are well-established credentials that were developed by two separate industry organizations, namely $(ISC)^2$ and ISACA, respectively. CISSP is a highly coveted certification that often serves as a prerequisite for cybersecurity leadership roles; it covers both technical and managerial concepts in cybersecurity. CISA is commonly held by professionals who perform or oversee IT audits, such

as those required by SOX. Collectively, these credentials should provide us with substantial breadth and depth for comparison.

In addition to CISSP and CISA, we have outlined the general requirements for the Certified Public Accountant credential, which will serve as a practical analog for ACFE for comparison. While a variety of positions and experiences may lead to ACFE designation, the CPA directly satisfies many of the ACFE requirements and serves as a prerequisite for some of the roles that can lead to becoming an ACFE (e.g., Certified Public Accountant, Auditor, Principal Accounting Officer, etc.) Academic literature has established that CPAs would "easily meet" the criteria for ACFE, and audit committee members who hold CPA licenses are highly likely to be designated as financial experts at their respective organizations.[52] We can evaluate these requirements to further define the ideal qualifications for cybersecurity expertise at a more practical, tangible level.

[52] Tom Wilson, "WHAT DISTINGUISHES AUDIT COMMITTEE FINANCIAL EXPERTS FROM OTHER AUDIT COMMITTEE MEMBERS?," n.d.

Table 8 - CISSP vs. CISA vs. CPA

Table 8: CISSP vs. CISA vs. CPA			
Credential:	**CISSP**[53]	**CISA**[54]	**CPA**[55]
Work Experience:	Six years of work experience within two or more of the eight domains of the (ISC)² CISSP CBK: 1. Security and Risk Management 2. Asset Security 3. Security Architecture and Engineering 4. Communication and Network Security 5. Identity and Access Management (IAM) 6. Security Assessment and Testing 7. Security Operations 8. Software Development Security	Five years of work experience in information systems auditing, control, or security	One year of work experience involving "the use of accounting, attest, compilation, management advisory, financial advisory, tax or consulting skills which were gained through employment in government, industry, academia or public practice."
Education:	None specifically required for exam, apart from Continuing Professional Education courses	None specifically required for exam, apart from Continuing Professional Education courses	Bachelor's degree with specific coursework requirements
Substitutions:	One year of work experience may be substituted for one of the following: • A four-year college degree or regional equivalent • An advanced degree in information security • An approved credential, such as CISA	A maximum of three years of work experience may be waived through specific formal education or general work experience in audit or information systems	Generally N/A
Examination:	Comprehensive examination	Comprehensive examination	Comprehensive examination

[53] "CISSP Experience Requirements," accessed April 22, 2023, https://www.isc2.org:443/Certifications/CISSP/Experience-Requirements.
[54] "Earn a CISA Certification," ISACA, accessed April 22, 2023, https://www.isaca.org/credentialing/cisa/get-cisa-certified.
[55] "CPA Requirements By State - Beat the CPA! 2023," accessed April 23, 2023, https://beatthecpa.com/cpa-requirements-by-state/.

6.2 – Recommendations for Work Experience

In addition to requiring a certain amount of experience, the CISSP, CISA, and CPA require experience in specific professional domains. The CISSP is generally the most prescriptive, requiring experience in at least two of eight specific information security domains. The rationale for requiring experience in multiple domains is likely to expand the candidate's breadth of exposure to cybersecurity. Meanwhile, the CISA and CPA requirements are relatively broad, requiring experience that can be drawn from a handful of relevant fields.

Notably, all three exams require the verification of work experience. CISSP requires that candidates are endorsed by a current CISSP holder who can vouch for the candidates' security experience, or individuals can pursue endorsement from $(ISC)^2$ itself.[56] The CISA certification process does not utilize a mechanism for peer endorsement; instead, supervisors must sign an experience attestation form, which the candidate will submit to ISACA for verification.[57] For CPA licensure, the prerequisite work experience generally must be supervised and signed off by a current CPA, who submits it to the state board or other governing body.

When looking at Table 8, we can observe that the CISSP, CISA, and CPA credentials require a certain number of years of experience for qualification. As such, it may be prudent for boards to consider directors with experience at or beyond the CISSP and CISA minimum requirements. However, while the CISSP and CISA credentials technically allow candidates to partially reduce their years of experience through the completion of academic degrees or related

[56] "Endorsement | Online Endorsement Application | $(ISC)^2$," accessed April 23, 2023, https://www.isc2.org:443/Endorsement.
[57] "Earn a CISA Certification."

certifications, these substitutions may not be suitable in the context of cybersecurity expertise due to the exceptionally high level of responsibility bestowed upon corporate directors.

6.3 – Recommendations for Education

The CISSP and CISA exams do not have formal academic requirements, but certain degrees or certifications may count towards some of the required work experience. For example, $(ISC)^2$ has a policy that allows candidates to waive one year of work experience if they possess a "four-year college degree or regional equivalent" or an "advanced degree in information security from the U.S. National Center of Academic Excellence in Information Assurance Education (CAE/IAE)."[58] The CISSP certification also includes a provision that a portion of the work experience requirement may be waived if a candidate holds one of the certifications found on a specific list published by $(ISC)^2$. Meanwhile, CPA candidates are expected to complete at least 150 units of college coursework for licensure in most states.[59]

In the context of formal educational requirements, it may be beneficial for boards to seek out candidates who hold an information security degree, at the bachelor's level or higher, from an institution recognized as a National Center of Academic Excellence (NCAE). NCAE is a "collaborative cybersecurity educational program with community colleges, colleges, and universities that:

- Establishes standards for cybersecurity curriculum and academic excellence,
- Includes competency development among students and faculty,
- Values community outreach and leadership in professional development,

[58] "CISSP Experience Requirements."
[59] "CPA Requirements By State - Beat the CPA! 2023."

- Integrates cybersecurity practice within the institution across academic disciplines,
- Actively engages in solutions to challenges facing cybersecurity education."[60]

NCAE is widely recognized in the field of cybersecurity education, akin to government accreditation. As such, there is a presumed level of baseline competence, structure, and rigor imparted by CAE-designated curricula. The NCAE program spans various academic levels, ranging from community colleges to graduate schools, which puts a high-quality cybersecurity education within reach for many people. In the absence of an information security degree, boards may want to consider candidates with degrees in related academic disciplines from accredited schools, along with industry certifications.

For cybersecurity expertise, boards may consider utilizing the U.S. Department of Defense (DoD) 8570 standard for evaluating cybersecurity certifications. The 8570 standard has longstanding precedence within the U.S. DoD, which is "the world's biggest enterprise network."[61] The U.S. Department of Defense has evaluated many cybersecurity certifications and has prescribed several acceptable options under 8570, requiring certain employees to possess these certifications as a condition of employment. Generally, these certifications are divided into three levels, with Level III certifications aligning with the highest level of professional responsibility and cybersecurity experience within the DoD. As a point of reference, roles that fall under Level III often require 7-10 years of relevant experience. Both CISA and CISSP

[60] "National Centers of Academic Excellence," accessed April 23, 2023, https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.
[61] "DoD IT Environment Way Forward - DISTRO (Aug 2016).Pdf," accessed April 26, 2023, https://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf.

qualify as approved Level III certifications within the DoD.[62] Boards can review 8570 and utilize the DoD's methodologies and considerations to guide executive-level decision-making.

6.4 – Recommendations for Knowledge, Skills, and Abilities

For CISSP, $(ISC)^2$ requires candidates to have a solid understanding of the $(ISC)^2$ Common Body of Knowledge (CBK), which is a "peer-developed compendium of what a competent professional in their respective field must know, including the skills, techniques and practices that are routinely employed". Mastery of the $(ISC)^2$ CBK, as evidenced by passing certifications such as CISSP, demonstrates competence in the "most critical aspects of information security."[63] CISA also touches upon fundamental knowledge of information systems. However, the exam reference materials may not be as robust and comprehensive as the $(ISC)^2$ Common Body of Knowledge and differs in scope in some regards. CPA KSAs are relatively broad when derived from work experience, but the Uniform CPA Exam requires specific knowledge of accounting concepts.[64] Boards can evaluate CISSP and CISA reference materials to better understand the baseline KSAs needed for success as a cybersecurity leader. Boards can subsequently consider these KSAs while evaluating "cyber expert" candidates.

[62] "DoD Approved 8570 Baseline Certifications – DoD Cyber Exchange," accessed April 23, 2023, https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/.
[63] "$(ISC)^2$ CBK | Common Body of Knowledge," accessed April 26, 2023, https://www.isc2.org:443/Certifications/CBK.
[64] "Everything You Need to Know about the CPA Exam," accessed April 26, 2023, https://www.aicpa-cima.com/resources/toolkit/cpa-exam.

Areas of Future Research:

In future academic endeavors, the breadth of analysis can be expanded to cover other professional credentials, such as the ISACA Certified Information Security Manager (CISM) certification and NACD Directorship Certification, to provide deeper insights into ideal qualifications and areas of emphasis. Comparative analysis can also be expanded beyond ACFE and Cybersecurity Expertise into other domains, such as the evaluation process for professional witnesses and related legal precedent. The SEC cybersecurity expertise regulations will likely be implemented soon after the release of this paper, which may lead researchers to evaluate the market's reaction to these regulations, performing further analysis of the actual preparation level of boards as well as the scope and extent of disclosures being made regarding cybersecurity expertise.

Future research may also cover relevant topics, such as Directors and Officers liability insurance and how board cyber expertise may factor into litigation stemming from alleged breaches of fiduciary duty. Furthermore, the SEC should conduct further research and refine the Cybersecurity Expertise guidelines to include greater specificity in several areas. Public-Private Partnerships should also collaborate to explore topics of discussion within this domain, such as creating unified CBKs for reference.

Conclusion:

In summary, we have identified the key requirements for ACFE and Cybersecurity Expertise through comparative analysis, mapping both designations to the categories of "Work Experience", "Education", and "Knowledge, Skills, and Abilities". We subsequently derived numerous insights from these designations, which will hopefully assist boards with defining the minimum requirements for cybersecurity expertise. Some notable recommendations include leveraging industry certifications and Common Bodies of Knowledge to assess candidates, considering the scope and extent of a candidate's past work experience in relation to expected board member responsibilities, and recommending that candidates have knowledge regarding the practical application of cybersecurity standards and best practices.

We also explored several professional credentials, namely the CISSP, CISA and CPA, to further establish a fundamental understanding of the qualifications for cybersecurity expertise. The evaluation of these credentials led to several recommendations regarding the assessment of director qualifications, especially regarding measures of work experience and academic preparation for leadership. These efforts will hopefully lead to improved cybersecurity governance within publicly traded companies, which may protect consumers and shareholders from harm.

Works Cited:

"17 CFR Chapter II -- Securities and Exchange Commission." Accessed April 4, 2023. https://www.ecfr.gov/current/title-17/chapter-II.

"2022 NACD Public Company Board Practices and Oversight Survey." Accessed April 8, 2023. https://www.nacdonline.org/insights/publications.cfm.

AICPA. "Adopting the Comprehensive Definition of Attest: Protecting the Public." Accessed April 18, 2023. https://us.aicpa.org/content/dam/aicpa/advocacy/state/downloadabledocuments/what-are-attest-services.pdf.

"An Overview of Sarbanes-Oxley for the Information Security Professional | SANS Institute." Accessed April 21, 2023. https://www.sans.org/white-papers/1426/.

"Audit Committee Role & Responsibilities." Accessed April 11, 2023. https://www.cfainstitute.org/en/advocacy/issues/audit-committee-role-practices.

"Board-of-Directors-Cyber-Attitudes.Pdf." Accessed April 22, 2023. https://cams.mit.edu/wp-content/uploads/Board-of-Directors-Cyber-Attitudes.pdf.

"CF Disclosure Guidance: Topic No. 2 - Cybersecurity." Accessed April 4, 2023. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm#_ednref2.

"CISSP Experience Requirements." Accessed April 22, 2023. https://www.isc2.org:443/Certifications/CISSP/Experience-Requirements.

"CPA Requirements By State - Beat the CPA! 2023." Accessed April 23, 2023. https://beatthecpa.com/cpa-requirements-by-state/.

"Cyber Incident Reporting: New Rules, New Timelines | Crowe LLP." Accessed April 22, 2023. https://www.crowe.com/cybersecurity-watch/cyber-incident-reporting-new-rules-new-timelines.

"Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." Accessed April 4, 2023. https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

Deb, Debabrata. "Cyber Security Certification vs Degree: Which Is Best for Your Career?" ITPro, February 15, 2023. https://www.itpro.com/business-strategy/careers-training/370054/cyber-security-certification-vs-degree.

Deloitte United States. "Audit Committee Requirements." Accessed April 8, 2023. https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/audit-committee-requirements.html.

Deloitte United States. "Cybersecurity and Internal Audit." Accessed April 8, 2023. https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html.

"DoD Approved 8570 Baseline Certifications – DoD Cyber Exchange." Accessed April 23, 2023. https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/.

"DOD Cybersecurity Incident Reporting 062421 Cleared for Public Release AFRL-2021-2004, 25 Jun 2021_1.Pdf." Accessed April 22, 2023. https://www.safcn.af.mil/Portals/64/DOD%20Cybersecurity%20Incident%20Reporting%20062421%20Cleared%20for%20Public%20Release%20%20AFRL-2021-2004%2C%2025%20Jun%202021_1.pdf.

"DoD IT Environment Way Forward - DISTRO (Aug 2016).Pdf." Accessed April 26, 2023. https://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf.

"Endorsement | Online Endorsement Application | (ISC)^2." Accessed April 23, 2023. https://www.isc2.org:443/Endorsement.
"Everything You Need to Know about the CPA Exam." Accessed April 26, 2023. https://www.aicpa-cima.com/resources/toolkit/cpa-exam.
"FORM 10-K SolarWinds Corporation." Accessed April 25, 2023. https://www.sec.gov/Archives/edgar/data/1739942/000173994222000020/swi-20211231.htm.
Gartner. "Definition of Internal Controls - Gartner Finance Glossary." Accessed April 11, 2023. https://www.gartner.com/en/finance/glossary/internal-controls.
"Generally Accepted Accounting Principles (GAAP) Guide Sheet," n.d.
Investopedia. "GAAP: Understanding It and the 10 Key Principles." Accessed April 11, 2023. https://www.investopedia.com/terms/g/gaap.asp.
ISACA. "Earn a CISA Certification." Accessed April 22, 2023. https://www.isaca.org/credentialing/cisa/get-cisa-certified.
"(ISC)^2 CBK | Common Body of Knowledge." Accessed April 26, 2023. https://www.isc2.org:443/Certifications/CBK.
Kanji, Hetal, Orla Cox, and Simon Onyons. "Building Effective Cybersecurity Governance." *The Harvard Law School Forum on Corporate Governance* (blog), November 10, 2022. https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/.
King, Antoinette. "Cybersecurity Risk Is Business Risk." Industrial Cybersecurity Pulse, December 28, 2021. https://www.industrialcybersecuritypulse.com/facilities/cybersecurity-risk-is-business-risk/.
Muccini, Julia. "Cybersecurity Experience Disclosure | SEC Disclosure Requirement." *OCD Tech* (blog), March 21, 2022. https://ocd-tech.com/2022/03/21/sec-proposed-rule-could-add-cybersecurity-to-the-boardroom/.
"National Centers of Academic Excellence." Accessed April 23, 2023. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.
NetSuite.com. "Why Is Financial Reporting Important?" Oracle NetSuite, June 1, 2022. https://www.netsuite.com/portal/resource/articles/accounting/financial-reporting.shtml.
"POSSIBLE REVISIONS TO AUDIT COMMITTEE DISCLOSURES." Accessed April 8, 2023. https://www.sec.gov/rules/concept/2015/33-9862.pdf.
Rights (OCR), Office for Civil. "Breach Notification Rule." Text. HHS.gov, September 14, 2009. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
———. "What Does the Security Rule Require a Covered Entity to Do to Comply with the Security Incidents Procedures Standard?" Text. HHS.gov, April 8, 2010. https://www.hhs.gov/hipaa/for-professionals/faq/2002/what-does-the-security-rule-require-a-covered-entity-to-do-to-comply/index.html.
"SEC Issues Final Rules on Disclosure of Audit Committee Financial Experts and Codes of Ethics," n.d.
"SEC.Gov | About the SEC." Accessed April 4, 2023. https://www.sec.gov/strategic-plan/about.
"SEC.Gov | Investor Bulletin: An Introduction to The U.S. Securities and Exchange Commission – Rulemaking and Laws." Accessed April 4, 2023. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_rulemaking.

"SEC.Gov | SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." Accessed April 15, 2023. https://www.sec.gov/news/press-release/2022-39.

Sikora, Ted. "Director Perspective: Top Priorities of 2023." *The Harvard Law School Forum on Corporate Governance* (blog), February 10, 2023. https://corpgov.law.harvard.edu/2023/02/10/director-perspective-top-priorities-of-2023/.

Sloan, Rob. "Analyzing Board-Level Cybersecurity Experience." WSJ. Accessed April 3, 2023. https://www.wsj.com/articles/analyzing-board-level-cybersecurity-experience-11669674866.

———. "Survey Finds Boards Have Work To Do on Cybersecurity: Executive Summary." WSJ. Accessed April 8, 2023. https://www.wsj.com/articles/survey-finds-boards-have-work-to-do-on-cybersecurity-executive-summary-6cf47acb.

———. "Survey Results Part One: Board Directors Have Work To Do on Cybersecurity." WSJ. Accessed April 3, 2023. https://www.wsj.com/articles/survey-results-part-one-board-directors-have-work-to-do-on-cybersecurity-697223d0.

"The Laws That Govern the Securities Industry | Investor.Gov." Accessed April 4, 2023. https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#sox2002.

Walker, Brian. "Council Post: 90% Of Boards Are Not Ready For SEC Cyber Regulations." Forbes. Accessed April 2, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/02/06/90-of-boards-are-not-ready-for-sec-cyber-regulations/.

Wilson, Tom. "WHAT DISTINGUISHES AUDIT COMMITTEE FINANCIAL EXPERTS FROM OTHER AUDIT COMMITTEE MEMBERS?," n.d.