# Evaluating the Effectiveness of Third-Party Cyber Threat Intelligence In Supporting Cyber Regulatory Readiness

by

Byron Busby

---

Doctoral Research Project

Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

---

California Intercontinental University

2025

**Evaluating the Effectiveness of Third-Party Cyber Threat Intelligence In Supporting Cyber Regulatory Readiness**

by

Byron Busby

Doctoral Research Project – Case Study

Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

California Intercontinental University

2025

| | |
|---|---|
| Byron Busby, Doctoral Candidate | September 16, 2026 |
| Dr. Pedro Nunes, Research Chair | September 16, 2026 |
| Dr. Robert Neely, Chief Academic Officer | September 16, 2026 |

**Acknowledgements**

*"It takes a village to raise a child."* — African Proverb

A dissertation carries one name on its title page, but this one was never carried by one person alone. It was built, sustained, and finished by a village — the people who believed this was possible before I fully did, who made room for it in my life, and who each, in their own way, planted a seed that grew into this body of work.

To my chair, Dr. Pedro Nunes, thank you for your rigor, your patience through every round of revisions, and your refusal to let good enough stand in for excellent. This project is sharper, more honest, and more defensible because of your guidance, and I am a better scholar for having worked under it. To the members of my committee, thank you for the time, scrutiny, and care you gave to this work — your questions and feedback made it stronger.

To my colleagues and professional network — the mentors who opened doors, the peers who talked through ideas with me at odd hours, and the practitioners who generously gave their time and candor as participants in this study, thank you for trusting this work with your experience and expertise. This research exists because you were willing to be part of it.

To my friends and family, thank you for the check-ins, the encouragement, and the grace you extended every time I simply said, "I can't, I'm busy, or I'm unable to…". Your friendship carried me through the parts of this process that no methodology chapter can capture.

To my brother, Ray, I am deeply grateful and owe you a profound debt of gratitude for being my steadfast supporter and constant protector throughout every chapter of my life. You gave me the opportunity to become the Uncle I always aspired to be, blessing me with a niece and nephews, whom I strive daily to serve as a role model, to encourage, to lead by example, and to be a source of inspiration.

To my parents, Arthur & Ann, thank you for instilling in me the discipline and belief that made a doctorate feel like a reasonable thing to attempt in the first place. Long before I understood what a doctorate was, you both modeled for me what it means to work toward something bigger than yourself and to do so with integrity. Every late writing task, every setback I pushed through, every moment I refused to quit — that was you, showing up in me. This achievement bears your name even though it isn't printed there. Thank you for giving me the roots that made this possible and ultimately for the nurturing village you surrounded me with.

To Lincoln, Parker, and Clarke, thank you for being patient with me through every night I sat at my laptop instead of sitting with you, and for every "just give me a few more minutes." You are the reason I started this journey, and you were my motivation on the days I did not feel like finishing it. I hope this shows you that it is never too late to chase something hard, and that finishing what you start is worth every late night it costs. Thank you for sharing countless encouraging hugs. Everything I chased in these pages, I chased with you in mind — and I hope one day you chase something of your own with the same stubbornness I chased this.

To Chaunte, thank you for carrying so much of what I could not carry while I disappeared into research, transcripts, coding, and revisions for hours I cannot get back. No version of this doctorate exists without you. Your patience and steadiness gave me the room to finish and to demonstrate to our kids that anything is possible with dedication, persistence, and a supportive backbone. I know that sacrifice does not show up anywhere in these pages, but it is in every one of them. This degree bears my name, but it was built on your patience, your steadiness, and your love.

Furthermore, to everyone whose name does not appear above but whose encouragement, prayer, advice, or simple belief in me became part of the foundation this dissertation stands on — thank you. You are the village. This accomplishment is as much yours as it is mine.

## Abstract

The governance of cybersecurity risk in large, complex financial institutions has become a central preoccupation for regulators, boards, and senior leadership alike. Regulatory bodies, including the Basel Committee on Banking Supervision and the National Institute of Standards and Technology, have progressively elevated the evidentiary standard required during supervisory examinations, shifting away from control-checklist approaches toward outcome-oriented assessments that demand traceable decision rationale, board-level accountability, and sustained governance rigor (BCBS, 2021; NIST, 2024). This evolution has reframed regulatory readiness not as a periodic compliance exercise but as a continuous organizational capability that must be evidenced through governance routines, information artifacts, and leadership accountability structures that can withstand intensive examiner scrutiny.

In response to these intensifying demands, many institutions have substantially expanded their reliance on third-party cyber threat intelligence (CTI) providers and vendor-supported regulatory readiness services, seeking to supplement internal capabilities without proportionate growth in staffing or specialized expertise (Gartner, 2023; PwC, 2025). However, despite the scale of this investment, the literature provides limited empirical evidence on how organizational decision-makers at regulated financial institutions assess whether these services meaningfully contribute to regulatory-readiness outcomes. This gap undermines confidence in compliance budgeting, vendor governance, and internal capability development decisions.

This qualitative single-case study explores how cybersecurity, risk, and compliance professionals at a large, U.S.-based, globally systemically important bank (G-SIB) evaluate the regulatory readiness of third-party CTI and vendor-supported services. Using semi-structured

interviews, purposive sampling, and thematic analysis, the study examines how decision-makers define and operationalize effectiveness within a regulatory context, how vendor investment decisions are justified, and how external intelligence is translated into governance processes and examination-ready documentation. The findings may inform more defensible vendor governance frameworks, strengthen evidence-based decisions on compliance investments, and contribute to the growing body of knowledge on cybersecurity governance in regulated financial environments.

*Keywords:* cyber threat intelligence, regulatory readiness, cybersecurity governance, qualitative single-case study, third-party vendors, globally systemically important bank

## Table of Contents

*Acknowledgements* ..... *iii*

*Abstract* ..... *v*

*List of Tables* ..... *ix*

*List of Figures* ..... *x*

*CHAPTER 1: Introduction to Doctoral Research Project* ..... *1*

**Background of the Problem & Problem Statement** ..... **3**

**Purpose Statement & Significance of the Study** ..... **4**

**Literature Support** ..... **6**

**Project Type & Organization Permission** ..... **7**

**Research Questions and Methodology** ..... **8**

*CHAPTER 2: Literature Support* ..... *10*

**Description of the Problem and Business Practices** ..... **10**

**Discussion on Previous Research** ..... **12**

**Research Framework** ..... **14**

**Summary of Literature Support** ..... **18**

**Complete Literature Review** ..... **20**

*Chapter 3: Research Methodology* ..... *27*

**Discussion on the Population and Sampling** ..... **30**

**Data Collection and Data Analysis** ..... **32**

**Assumptions, Limitations, and Delimitations ..... 37**

***CHAPTER 4: Results, Discussions, and Implications ..... 40***

**Implications and Recommendations for Future Research ..... 81**

**Summary and Study Conclusion ..... 89**

***References ..... 92***

***Appendix A: List of Acronyms ..... 99***

***Appendix B: Qualitative Data Analysis Procedures ..... 100***

***Appendix C: Project Type & Organization Permission ..... 101***

***Appendix D: Research Design Alignment Matrix ..... 102***

***Appendix E: Semi-Structured Interview Protocol ..... 104***

***Appendix F: Preliminary Qualitative Coding Framework ..... 106***

## List of Tables

Table 3.1. Coding Structure for Thematic Analysis ……35

Table 3.2. Research Question Alignment Matrix ……36

Table 4.1. Participant Characteristics (N = 18) ……..……46

Table 4.2. Thematic Structure Overview …….……...51

Appendix D. Research Design Alignment Matrix …….….96

## List of Figures

Figure 1.1 Conceptual Framework for Evaluating the Regulatory Readiness Value of Third-Party Cyber Threat Intelligence ……..……...…….16

Figure 4.1. Screening-Survey Frequency of Reliance on Vendor-Provided Threat Intelligence or Advisory Services (N = 39) ……...……48

Figure 4.2. Screening-Survey Extent of Responsibility Evaluating or Interpreting Vendor-Supplied Intelligence (N = 39) ……..……49

Figure 4.3. Thematic Prevalence Across the Interview Sample ……....52

# CHAPTER 1: Introduction to Doctoral Research Project

Large federally regulated financial institutions occupy a distinctive and consequential position in the cybersecurity governance landscape. Organizations designated as globally systemically important banks (G-SIBs) operate under consolidated supervisory frameworks administered by multiple federal regulatory bodies and face examination standards that have grown considerably more demanding over the preceding decade. Regulatory authorities—including the Basel Committee on Banking Supervision, the Federal Financial Institutions Examination Council, and the Office of the Comptroller of the Currency—have progressively shifted their evaluation criteria from the presence of cybersecurity controls to the documented effectiveness, traceability, and governance accountability with which those controls are managed over time (BCBS, 2021; NIST, 2024). This shift has elevated cybersecurity preparedness from a technical compliance function to an enterprise governance capability that boards, senior executives, and examiners now evaluate with sustained and detailed scrutiny.

In response to these expectations, many large financial institutions have substantially expanded their use of third-party cyber threat intelligence (CTI) providers and vendor-supported regulatory readiness services. These services encompass a range of functions, including continuous threat monitoring, regulatory control mapping, preparation of examination documentation, and advisory guidance during supervisory reviews. Industry reports indicate that global investment in cybersecurity risk and compliance services continues to climb as institutions seek to keep pace with rapidly evolving threats and regulatory requirements without a proportionate increase in internal staffing (Gartner, 2023; PwC, 2025).

A fundamental governance problem persists beneath this investment, however. Cybersecurity and compliance leaders within regulated institutions must justify significant, recurring vendor expenditures without clear, outcome-based evidence that external intelligence and readiness services consistently and defensibly improve regulatory preparedness. Regulatory readiness is not simply a product of access to sophisticated threat data; it requires translating external intelligence into governance-ready artifacts—control assessments, risk prioritization narratives, documentation packages—that satisfy examiner expectations for traceability, consistency, and internal oversight (BCBS, 2021; Ainslie et al., 2023). Intelligence that is technically credible but organizationally disintegrated may fail to support examination preparation regardless of its operational quality.

This challenge is particularly consequential within G-SIB institutions, which maintain extensive third-party vendor ecosystems, are subject to simultaneous oversight from multiple federal regulators, and face intensive, frequent examination cycles. When cybersecurity and compliance leaders cannot articulate a clear, evidence-based account of how vendor-provided intelligence strengthens readiness outcomes, the governance implications are serious: budgeting decisions are made on assumptions rather than evidence, vendor relationships are renewed without demonstrated value, and internal capability development may be deferred in favor of external dependency (Li et al., 2021; McNulty, 2023).

This doctoral research project addresses this applied governance problem by investigating how cybersecurity, risk, and compliance professionals within a large, U.S.-based, globally systemically important bank (G-SIB) evaluate the regulatory-readiness value of third-party CTI and vendor-supported services. Using a qualitative single-case study design, the study examines how these professionals define and assess effectiveness in a regulatory context, how vendor-

provided intelligence is integrated into readiness planning and governance processes, and what challenges they encounter in translating external intelligence into examination-ready evidence.

## Background of the Problem & Problem Statement

Cybersecurity regulatory oversight of large financial institutions has undergone a sustained and consequential evolution over the preceding two decades. Federal regulatory authorities now expect G-SIB institutions to demonstrate not merely the existence of cybersecurity controls but their ongoing operational effectiveness, alignment with enterprise risk governance, and traceability across examination cycles (BCBS, 2021; NIST, 2024). This shift reflects a broader transformation in supervisory philosophy: regulators increasingly evaluate institutions not on the controls in place, but on how those controls are governed, documented, and held accountable to senior leadership. The practical result is that cybersecurity preparedness now implicates governance structures, information artifact quality, and the demonstrability of risk-informed decision-making at every organizational level (Li et al., 2021; McNulty, 2023).

Against this backdrop, many large financial institutions have embedded third-party CTI providers and vendor-supported readiness services into their core compliance and governance workflows. These vendors offer access to specialized threat data, regulatory benchmarking, control mapping assistance, and examination preparation support that institutions would otherwise need to develop and maintain internally—a proposition frequently attractive given persistent workforce constraints and the rapid pace of regulatory change (Gartner, 2023; Oshri et al., 2019). Both providers and industry discourse often position vendor-supported services as essential components of modern cybersecurity governance infrastructure.

The specific problem this study addresses is that large, federally regulated financial institutions may lack defensible, outcome-based evidence to demonstrate whether costly third-party CTI and vendor-supported regulatory-readiness services meaningfully improve preparedness for cybersecurity regulatory examinations. In the absence of such evidence, investment decisions are made based on perceived necessity, vendor assurance, or industry precedent rather than demonstrated effectiveness—a pattern that risks perpetuating escalating compliance expenditures without commensurate improvements in examination outcomes, governance defensibility, or organizational resilience (PwC, 2025; Oshri et al., 2019).

## Purpose Statement & Significance of the Study

The purpose of this qualitative single-case study is to explore how cybersecurity, risk, and compliance professionals within a large, U.S.-based, globally systemically important bank (G-SIB) evaluate the regulatory-readiness value of third-party cyber threat intelligence (CTI) and vendor-supported services. The participating institution is headquartered in New York. It is subject to consolidated supervision by the Federal Reserve Board, examination authority of the Office of the Comptroller of the Currency (OCC), and oversight by the Consumer Financial Protection Bureau (CFPB). The institution operates across more than 160 countries, employs one of the largest enterprise cybersecurity governance programs in the financial services industry, and is subject to annual supervisory examinations and stress testing requirements under the Dodd-Frank Wall Street Reform and Consumer Protection Act (2010). The organization is not named in this study to preserve participant confidentiality and comply with the institution's data governance requirements.

This study is not designed to test hypotheses or establish statistical relationships between variables. Its scope is deliberately bounded: the study does not seek to produce findings generalizable across the entire participating institution, its globally distributed branch network, or the broader financial sector. Such generalization would not be an appropriate evaluative standard for a qualitative single-case study design (Yin, 2018; Hancock et al., 2021). Rather, the study pursues analytical generalization — the extension of empirically grounded findings to governance theory and cybersecurity compliance practice — which is the recognized contribution that qualitative single-case study methodology is designed and validated to produce (Yin, 2018; Creswell & Creswell, 2023; Hancock et al., 2021).

Its purpose is to develop a rich, contextualized, and analytically supported understanding of how experienced governance professionals interpret, assess, and operationalize third-party CTI in response to the specific governance and regulatory demands of a G-SIB institution. Data will be gathered through semi-structured interviews with professionals responsible for cybersecurity governance and regulatory readiness. A purposive sampling strategy will ensure participants possess the professional depth required to address the research questions substantively. Interview data will be analyzed using the six-phase thematic analysis procedure described by Braun and Clarke (2022) to identify patterns in how vendor-supported intelligence is evaluated, integrated, and assessed against regulatory readiness criteria.

The significance of this study is predominantly threefold. First, it addresses a documented gap in the empirical literature on cybersecurity governance: while third-party CTI and vendor-supported services have become embedded in the compliance strategies of large financial institutions, scholarly work on how these services are evaluated against regulatory-readiness criteria remains limited (Ainslie et al., 2023; Li et al., 2021; Zibak et al., 2022). Second, the study

contributes to theoretical development at the intersection of information governance, regulatory governance, and dynamic capabilities frameworks by examining how vendor-provided intelligence is interpreted and operationalized within governance-oriented contexts (Abraham et al., 2019; Coglianese & Lehr, 2019; Teece, 2019). Third, the findings carry direct practical relevance for senior cybersecurity leaders, GRC professionals, and compliance officers responsible for vendor selection, investment justification, and governance accountability within highly regulated institutional environments. Furthermore, the study provides a foundation for future research exploring alternative readiness models — including internally developed or artificial intelligence (AI)-enabled approaches — that contribute to more resilient and sustainable regulatory compliance practices in highly regulated financial environments.

## Literature Support

- Regulatory bodies governing large financial institutions have progressively raised examination standards, moving from control-presence verification to outcome-oriented assessments that demand documented governance accountability, traceable risk decision-making, and board-level oversight of cybersecurity activities (BCBS, 2021; NIST, 2024).
- Global investment in cybersecurity threat intelligence and vendor-supported compliance services continues to grow substantially; however, organizations frequently struggle to demonstrate the regulatory-readiness value of these expenditures or to connect vendor outputs to measurable examination outcomes (Gartner, 2023; PwC, 2025).
- Research in cybersecurity governance identifies CTI as operationally valuable but consistently underscores that its contribution to regulatory preparedness—specifically

examination readiness, documentation quality, and governance defensibility—remains empirically underexplored (Ainslie et al., 2023; Zibak et al., 2022).

- The outsourcing and third-party risk literature highlights that vendor dependence introduces governance risks when clarity of accountability, internal validation routines, and organizational capability development are weakened; in regulated environments, institutions remain fully accountable for compliance outcomes regardless of how services are organized (Oshri et al., 2019; BCBS, 2021).

## Project Type & Organization Permission

This study is a qualitative single-case study conducted within a large, U.S.-based, globally systemically important bank (G-SIB), headquartered in New York. The institution is subject to consolidated oversight by the Federal Reserve Board, examination authority of the OCC, and supervisory jurisdiction of the CFPB. It operates within the regulatory scope of the Dodd-Frank Wall Street Reform and Consumer Protection Act (2010). Its scale, regulatory complexity, and extensive third-party vendor ecosystem make it an analytically appropriate, information-rich research site for examining how external intelligence is evaluated in governance and regulatory readiness processes.

The institution is not identified by name in this study. Organizational permission to conduct research has been requested and is pending final academic approval. The study will not access proprietary systems, confidential client data, or non-public regulatory examination materials. All data will be collected through voluntary, IRB-approved participant interviews, and no sensitive operational information will be solicited or reported.

## Research Questions and Methodology

### *RQ1: Perception of Effectiveness*

How do cybersecurity and compliance professionals within a large, federally regulated U.S. financial institution perceive the effectiveness of third-party threat intelligence in supporting regulatory readiness?

This question directly addresses the evidentiary gap identified in the problem statement. Rather than assuming that third-party CTI improves regulatory preparedness, RQ1 investigates how effectiveness is defined, experienced, and evaluated by professionals with direct governance and examination responsibilities. The qualitative orientation of this question is deliberate: perceptions of effectiveness in complex regulatory contexts are shaped by institutional history, governance maturity, examiner expectations, and interpretive judgment—dimensions that cannot be reduced to numerical metrics.

### *RQ2: Vendor Influence on Governance Processes*

How do decision-makers describe the role of third-party vendors in influencing regulatory readiness planning, assessment consistency, and investment decisions?

RQ2 investigates the governance dimension of vendor reliance. By exploring how vendor-supported services shape planning processes and influence assessment decision-making, this question surfaces the mechanisms through which external intelligence either strengthens or complicates the governance routines that examiners evaluate. It also addresses the investment-justification problem: how decision-makers account for vendor contributions when making resourcing and procurement decisions.

### *RQ3: Challenges and Limitations*

What challenges or limitations do participants identify when using third-party threat intelligence for regulatory examination preparation?

RQ3 extends the inquiry to the practical barriers that constrain vendor intelligence from translating into regulatory preparedness outcomes. Understanding these challenges clarifies why increasing investment in third-party services does not automatically yield commensurate improvements in examination readiness—a pattern that the literature has theorized but not empirically documented in G-SIB institutional contexts.

# CHAPTER 2: Literature Support

## Description of the Problem and Business Practices

Large, federally regulated financial institutions operate at the intersection of intensifying cybersecurity regulatory demands and increasingly sophisticated threat environments. This convergence has elevated cybersecurity governance from a technical function to a board-level accountability concern. Regulatory authorities governing these institutions have progressively shifted their supervisory approach from prescriptive, checklist-oriented assessments to outcome-oriented evaluations that require institutions to demonstrate governance accountability, decision traceability, and documented oversight of cybersecurity risk management activities (BCBS, 2021; NIST, 2024). Examination outcomes are now shaped not only by the existence of cybersecurity controls but also by the quality of governance processes, documentation standards, and leadership oversight mechanisms that demonstrate how those controls are managed over time.

In response to these demands, many large financial institutions have embedded third-party CTI providers and vendor-supported regulatory readiness services into their core compliance and governance workflows. These services are engaged to support continuous threat monitoring, regulatory control mapping, documentation preparation for examinations, and advisory guidance during supervisory reviews. From an operational and strategic standpoint, outsourcing these functions offers access to specialized expertise and threat data that organizations may lack the internal capacity to develop and sustain at the required scale (Gartner, 2023; Oshri et al., 2019). Vendor-supported services are often presented by both providers and industry peers as efficient pathways to compliance maturity and examination readiness.

A critical governance problem arises when organizational leaders must justify continued or expanded investment in these external services without defensible, outcome-based evidence that they consistently and measurably improve regulatory readiness. Regulatory readiness depends not on the volume or sophistication of external intelligence consumed, but on the organization's capacity to translate that intelligence into auditable governance artifacts: control assessments, risk prioritization rationale, documentation packages, and oversight records that satisfy examiner expectations for traceability and defensibility (Abraham et al., 2019; Ainslie et al., 2023). External intelligence that is technically credible but organizationally disintegrated may fail to support examination preparation regardless of its operational quality.

This disconnect creates consequential uncertainty in cybersecurity investment decision-making. When leaders cannot clearly articulate whether vendor-provided intelligence strengthens governance outcomes, decisions regarding contract renewal, capability investment, and vendor oversight are made without a reliable evidentiary foundation (PwC, 2025; McNulty, 2023). For G-SIB institutions—where examination cycles are intensive, regulatory expectations are detailed, and the consequences of examination findings carry significant operational and reputational weight—this uncertainty is a material governance challenge, not merely an academic concern.

Although third-party CTI and vendor-supported readiness services have become standard features of large-institution compliance strategies, the empirical literature has prioritized their operational security benefits over their contribution to governance-oriented regulatory readiness (Ainslie et al., 2023; Zibak et al., 2022). The result is an evidence gap that leaves practitioners without the outcome-based knowledge needed to make defensible decisions about vendor reliance, internal capability development, and compliance investment priorities.

## Discussion on Previous Research

Prior research on CTI and third-party vendor reliance in regulated financial environments has developed along largely parallel and, in important respects, divergent trajectories. Research on CTI has matured considerably over the preceding decade, yielding systematic reviews, empirical studies, and conceptual frameworks that document the value of intelligence across strategic, operational, and tactical decision-making contexts (Ainslie et al., 2023; Wagner et al., 2019; Tounsi & Rais, 2018). This body of work establishes, with reasonable empirical consistency, that timely, relevant, and interpretable intelligence supports improved detection, triage, and incident response outcomes. What it does not adequately address is the translation challenge unique to regulatory environments: the requirement to convert intelligence outputs into auditable governance artifacts that demonstrate decision accountability and traceability of controls to external examiners.

Standard operationalizations of CTI value in existing research—detection speed, false positive rates, sharing participation, and incident frequency—do not map onto the governance defensibility constructs that supervisory examinations assess (Zibak et al., 2022; Cascavilla et al., 2021). As Ainslie et al. (2023) documented in their comprehensive review of CTI for security decision-making, the mechanisms by which intelligence outputs are integrated into organizational governance processes remain understudied, particularly in regulated institutional contexts where auditability and accountability are primary evaluation criteria.

The literature on IT outsourcing and vendor management presents a parallel limitation. Research in this domain has produced valuable insight into the efficiency gains, knowledge transfer dynamics, and governance risks associated with third-party service relationships (Oshri et al., 2019; Lacity & Willcocks, 2014). It is well established that vendor reliance can erode internal

governance capabilities, obscure accountability, and create concentration risks—risks that are amplified in regulated industries, where the regulated entity bears full compliance accountability regardless of the extent to which services are externally sourced (Oshri et al., 2019; BCBS, 2021). However, empirical studies examining how governance professionals evaluate vendor contributions against specific compliance outcomes—such as examination preparedness or documentation quality—remain rare.

A smaller but theoretically significant body of work has investigated cybersecurity disclosure and regulatory governance in financial institutions. Li et al. (2021) found that the specificity and consistency of cybersecurity governance disclosures shape how regulators and markets infer institutional preparedness, suggesting that information artifact quality—not the deployment of technical controls—is the primary lens through which supervisory assessments are formed. McNulty (2023) extended this analysis to the regulatory context, demonstrating that institutions are increasingly evaluated on their capacity to produce and steward high-quality governance information. These studies provide important theoretical grounding but do not address the operational question of how third-party CTI outputs are integrated into, and validated against, the documentation and governance routines that produce examination-ready evidence.

Collectively, the prior research offers robust theoretical foundations from information governance, dynamic capabilities, and regulatory theory traditions, but stops short of empirically examining the evaluative processes through which governance decision-makers within regulated financial institutions assess, validate, and operationalize third-party CTI within regulatory readiness workflows. This study is specifically designed to fill that empirical space.

## Research Framework

The appropriate organizing structure for this doctoral research project is a conceptual framework rather than a single theoretical framework. A theoretical framework is grounded in one or more established theories and is typically used to test, refine, or extend them within a particular empirical context (Ravitch & Carl, 2021). While this study draws on constructs from information governance theory (Abraham et al., 2019), regulatory governance theory (Coglianese & Lehr, 2019), and dynamic capabilities theory (Teece, 2019), no single existing theory adequately accounts for the multi-dimensional evaluative processes through which governance professionals within regulated financial institutions assess the regulatory-readiness value of third-party CTI in practice. A conceptual framework, by contrast, is developed through systematic synthesis of prior literature, professional practice insight, and the specific contours of the problem under investigation (Ravitch & Carl, 2021). It affords the analytical flexibility needed to model context-dependent relationships among vendor inputs, organizational actors, governance decision processes, and regulatory-readiness outcomes, while remaining anchored in relevant scholarship.

### *Importance of the Conceptual Framework*

The conceptual framework serves as the structural backbone of this study. It delineates the scope of inquiry—distinguishing external intelligence inputs from the internal evaluative and governance processes through which those inputs are interpreted and acted upon; clarifies the relationship pathways among vendor intelligence, organizational actors, governance decision-making, and regulatory readiness outcomes; guides interview protocol design by identifying constructs that participant responses should illuminate; and anchors data analysis in governance-oriented outcomes rather than operational performance proxies, preserving alignment with the study's applied DBA objectives. The framework is grounded in a well-established principle in

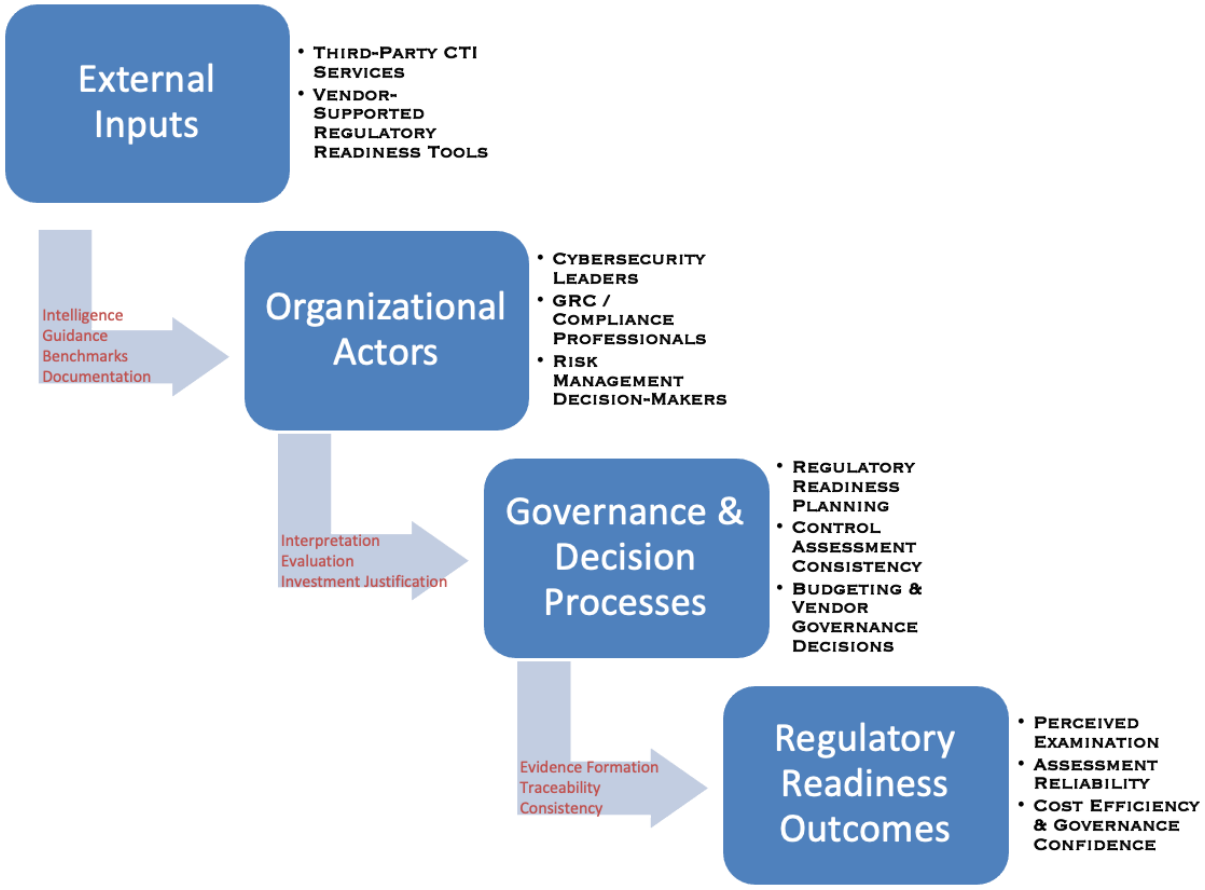
information systems and governance research: the value of information artifacts is not intrinsic to the artifact itself but is realized through the organizational processes of interpretation, validation, integration, and accountability through which those artifacts are engaged (Abraham et al., 2019; Tallon et al., 2013).

### *Conceptual Framework Diagram*

The conceptual framework illustrates how vendor-provided intelligence flows through organizational actors and governance decision processes to produce—or fail to produce—regulatory readiness outcomes.

**Figure 1.1**

*Conceptual Framework for Evaluating the Regulatory Readiness Value of Third-Party Cyber Threat Intelligence*




*Note.* Developed by the researcher.

The framework begins with third-party CTI services and vendor-supported regulatory readiness tools as the primary external inputs: threat intelligence reports, regulatory control mappings, benchmarking analyses, readiness assessments, and advisory services delivered during examination preparation. These inputs are positioned as inputs rather than outcomes, reflecting the scholarly consensus that external intelligence does not inherently generate governance value

independent of the organizational processes through which it is engaged (European Union Agency for Cybersecurity [ENISA], 2022; Ainslie et al., 2023). The second component consists of organizational actors—cybersecurity leaders, GRC professionals, and risk management decision-makers—who perform an indispensable interpretive function: translating technical intelligence into regulatory-relevant evidence, assessing whether vendor outputs support examination readiness, and justifying cybersecurity investment decisions within governance accountability structures (Abraham et al., 2019; Tallon et al., 2013). The third component captures the governance and decision-making processes through which intelligence inputs are operationalized: regulatory readiness planning, control assessments, compliance documentation development, vendor governance, and investment decision-making—the translation layer where uncertainty most frequently emerges (Ainslie et al., 2023; Oshri et al., 2019). The fourth component consists of regulatory readiness outcomes: perceived examination preparedness, assessment consistency, and governance defensibility—constructs that reflect the quality of governance processes rather than operational cybersecurity performance metrics (BCBS, 2021; ENISA, 2022; Li et al., 2021).

### *Interaction of Components and Connection to Literature*

The framework posits that third-party CTI influences regulatory readiness outcomes indirectly, through the mediating roles of organizational actors and governance processes. This indirect pathway aligns with prior scholarship, which emphasizes that external intelligence generates governance value only when it is integrated into mature, accountable governance mechanisms characterized by traceability, internal validation routines, and defensible decision-making (Gartner, 2023; PwC, 2025; Abraham et al., 2019). By explicitly modeling this pathway, the framework clarifies the applied problem: institutions may invest substantially in external intelligence without producing commensurate improvements in regulatory readiness if the

components of organizational interpretation and governance integration are underdeveloped or absent.

## Summary of Literature Support

The literature surveyed in support of this study spans four interconnected domains that together constitute the theoretical and empirical foundation for the research: regulatory readiness as an organizational governance capability; cyber threat intelligence maturation and its governance value; third-party vendor dependence and associated governance risks; and operational resilience alongside continuous assurance expectations. Across these domains, a consistent and consequential pattern emerges. Regulatory bodies governing large financial institutions have fundamentally reoriented their supervisory expectations, moving away from control-checklist compliance toward outcome-oriented assessments that evaluate governance accountability, decision traceability, and the quality of information artifacts produced to evidence cybersecurity oversight (BCBS, 2021; NIST, 2024; Li et al., 2021). This shift has elevated cybersecurity regulatory readiness from a technical compliance function to a board-level governance capability—one that must be continuously demonstrated, documented, and defended before examiners rather than achieved through periodic compliance exercises (Coglianese & Lehr, 2019; Caluwe et al., 2024; Abraham et al., 2019). Dynamic capabilities theory reinforces this framing by characterizing regulatory readiness as an adaptive organizational capability that requires sustained investment in governance sensing, integration, and transformation routines rather than a one-time control deployment (Teece, 2019; Hillmann & Guenther, 2021).

Within this governance context, the literature on CTI establishes clear operational value—timely, relevant intelligence demonstrably supports detection, triage, and incident response

outcomes—but consistently falls short of demonstrating how vendor-provided intelligence contributes to the governance defensibility and documentation quality that regulatory examinations require (Ainslie et al., 2023; Zibak et al., 2022; Wagner et al., 2019). Research in information governance emphasizes that the value of intelligence is not inherent in the artifact itself but is realized through the organizational routines of interpretation, validation, and accountability by which it is engaged (Abraham et al., 2019; Taddeo, 2019). CTI products are predominantly designed for operational security use cases. They are structurally misaligned with the governance artifact requirements of regulatory examination preparation—a gap the literature identifies but does not empirically resolve. The outsourcing and third-party risk literature compounds this concern by documenting that vendor dependence introduces governance risks when accountability clarity and internal capability development are weakened, risks that are amplified in regulated institutional environments where full supervisory accountability remains with the regulated entity regardless of how services are organized (Oshri et al., 2019; BCBS, 2021). Operational resilience frameworks further reinforce the governance integration imperative: continuous assurance depends on the quality and institutional ownership of the information artifacts through which compliance is evidenced across examination cycles, not merely on access to external intelligence (BCBS, 2021; Bernardo et al., 2024; McNulty, 2023). Taken together, the literature establishes strong theoretical grounding. However, it reveals a persistent and consequential empirical gap: how governance professionals within large, federally regulated financial institutions actually evaluate, validate, and operationalize third-party CTI against regulatory readiness criteria remains substantially unexplored. The following literature review develops each of these four themes in depth. It concludes by identifying the specific methodological limitations that motivate the qualitative, single-case design employed in this study.

## Complete Literature Review

Cybersecurity regulatory readiness has emerged as a prominent governance concern for large, federally regulated financial institutions as cyber risk increasingly intersects with operational continuity, systemic stability, and market confidence (Eisenbach et al., 2022; Didenko, 2020; Marotta et al., 2017). Scholarly analysis of supervisory practice describes a sustained shift from prescriptive rule-following toward risk-based, outcome-oriented evaluation that privileges accountability, decision traceability, and the demonstrability of governance over the deployment of technical controls alone (Coglianese & Lehr, 2019; Arena et al., 2019; McNulty, 2023). This evolution has reframed regulatory readiness as a continuous organizational capability evidenced through governance routines, information artifacts, and leadership accountability structures that withstand sustained examiner scrutiny.

This review synthesizes and critically evaluates scholarship across four themes that collectively frame the study's theoretical and empirical foundation: (a) regulatory readiness as an organizational governance capability, (b) CTI maturation and the governance value question, (c) third-party vendor dependence and governance risk, and (d) operational resilience and continuous assurance expectations. Each theme is examined in relation to the evidence gap motivating this study, and the review concludes with a synthesis of persistent methodological limitations that support the proposed qualitative single-case design.

### *Regulatory Readiness as an Organizational Governance Capability*

Scholarly treatment of cybersecurity regulatory readiness has converged around a governance-capability framing that departs markedly from earlier technical-compliance perspectives. Research in corporate governance and IT governance emphasizes that effective oversight requires the institutionalization of accountable decision rights, documented monitoring

processes, and repeatable escalation routines that produce evidentiary records suitable for external evaluation (De Haes et al., 2020; Caluwe et al., 2024; Tallon et al., 2013). Applied to cybersecurity contexts, this framing implies that examination readiness is strengthened by the quality and consistency of governance documentation, the clarity of risk prioritization rationale, and the traceability of decisions to accountable leadership—not by the volume or sophistication of security controls alone.

Regulatory governance scholarship reinforces this perspective by characterizing modern supervisory frameworks as legitimacy-seeking systems that evaluate regulated entities on their capacity to demonstrate accountability and maintain transparency in governance under examination (Coglianese & Lehr, 2019; Arena et al., 2019). Li et al. (2021) provided empirical support for this characterization, demonstrating that the specificity and internalization of cybersecurity governance disclosures are significant indicators that regulators and markets use to assess institutional preparedness. Information governance theory extends this insight by conceptualizing organizations as producers and stewards of information artifacts—reports, assessments, policies, and records—that link operational reality to governance claims (Abraham et al., 2019; Tallon et al., 2013; Bernardo et al., 2024). McNulty (2023) demonstrated that financial regulators are increasingly attentive to the infrastructure institutions use to produce, validate, and present compliance information.

Dynamic capabilities theory frames regulatory readiness as an adaptive capability that requires continuous sensing of emerging threats and regulatory changes, the deliberate integration of new intelligence into governance routines, and the iterative transformation of those routines in response to evolving supervisory expectations (Teece, 2019; Hillmann & Guenther, 2021). Regulatory frameworks have codified these expectations explicitly: BCBS principles for

operational resilience require institutions to demonstrate adaptive capacity through disruptive events, including cyber incidents (BCBS, 2021), while NIST CSF 2.0 introduced a dedicated governance function addressing organizational oversight, policy alignment, and leadership accountability (NIST, 2024)—marking formal regulatory recognition that governance processes are the primary locus of preparedness assessment.

### *Cyber Threat Intelligence: Maturation and the Governance Value Question*

The academic literature on CTI has matured substantially over the preceding decade, yielding systematic reviews, empirical studies, and conceptual frameworks that document the value of intelligence across multiple decision-making contexts (Ainslie et al., 2023; Wagner et al., 2019; Tounsi & Rais, 2018). CTI is broadly defined as analyzed information about actual or potential threats, structured to support decision-making at strategic, operational, or tactical levels (Ainslie et al., 2023; Sarker et al., 2020). Empirical evidence for CTI's operational value is reasonably consistent: timely, relevant intelligence has been associated with improved detection outcomes, more efficient triage, and stronger incident-response coordination in organizational contexts where intelligence is appropriately matched to decision-making needs (Sarker et al., 2020; Ainslie et al., 2023). However, research also identifies quality dimensions—accuracy, relevance, completeness, timeliness, and interpretability—that significantly condition this value and whose absence can reduce or negate intelligence's contribution to decision quality (Zibak et al., 2022; Ainslie et al., 2023).

Governance-oriented scholarship introduces a further dimension, particularly relevant to regulated financial institutions: intelligence value is not inherent in the intelligence artifact but is realized through organizational sensemaking, governance embedding, and accountability routines by which that artifact is engaged (Taddeo, 2019; Abraham et al., 2019). This distinction is

especially consequential in regulatory contexts where the demonstrability of governance—the capacity to show that intelligence was received, curated, validated, and acted upon in ways that are traceable and defensible—is as important as operational security impact. For third-party CTI to support regulatory readiness, institutions must demonstrate not only that vendor intelligence was consumed but that it was integrated into control assessments, risk prioritization, and governance documentation in ways that satisfy examiner accountability expectations (Ainslie et al., 2023; Abraham et al., 2019; Li et al., 2021). CTI products and services are predominantly designed for operational use cases rather than for producing governance-ready artifacts suitable for regulatory examination—a structural misalignment between CTI product design and regulatory documentation requirements that constitutes a significant, underexplored dimension of the governance value question.

### *Third-Party Vendor Dependence and Governance Risk*

The expansion of cybersecurity outsourcing in large financial institutions reflects a pragmatic response to persistent workforce constraints, rapidly evolving technical demands, and specialized expertise requirements (Oshri et al., 2019; Gartner, 2023). The outsourcing literature documents genuine efficiency benefits: access to specialized knowledge, economies of scale, and flexibility in capability deployment (Oshri et al., 2019). However, the same literature identifies significant governance risks amplified in regulated institutional contexts. Excessive reliance on third-party vendors can erode internal governance capability by displacing the organizational learning, risk ownership, and interpretive expertise that produce genuinely defensible compliance narratives (Oshri et al., 2019; Teece, 2019). When vendor-produced materials are used without adequate internal validation, contextualization, and integration with governance, institutions risk producing readiness documentation that reflects vendor outputs rather than institutional risk

judgment—a distinction that attentive examiners are trained to identify (Abraham et al., 2019; Li et al., 2021).

IT governance scholarship emphasizes that effective oversight requires clear decision rights, robust monitoring mechanisms, and accountable governance structures that apply equally to third-party service relationships as to internally delivered functions (De Haes et al., 2020; Caluwe et al., 2024). Regulatory frameworks are equally clear: the regulated institution bears full supervisory responsibility for compliance outcomes regardless of how services are organized (BCBS, 2021). In polycentric regulatory regimes governing G-SIB institutions, supervisory trust is built through demonstrated governance ownership—the capacity to demonstrate that risk decisions are made by accountable institutional actors who understand and can defend them before examiners (Coglianese & Lehr, 2019; Arena et al., 2019). From a dynamic capabilities perspective, the readiness value of vendor-supported services depends critically on whether they contribute to institutional capability building—enhancing the organization's sensing, integration, and transformation routines—rather than substituting for internal capability development (Teece, 2019; Hillmann & Guenther, 2021).

### *Operational Resilience and Continuous Assurance*

Operational resilience has emerged as a central organizing concept within financial regulatory frameworks, connecting cybersecurity governance, business continuity, and third-party risk management within a unified supervisory lens (Hillmann & Guenther, 2021; Eisenbach et al., 2022; Didenko, 2020). BCBS guidance requires financial institutions to demonstrate the capacity to deliver critical business services through disruptive events—including cyber incidents—at levels consistent with supervisory expectations for service continuity (BCBS, 2021). This requirement situates cybersecurity preparedness within a broader resilience governance

framework: institutions must show not only that they can prevent cyber incidents but that their governance processes enable effective response, recovery, and adaptation. Information governance research indicates that continuous assurance—the ongoing capacity to demonstrate compliance and governance quality across examination cycles—depends on the quality, consistency, and institutional ownership of the information artifacts through which monitoring, reporting, and evidence are produced (Abraham et al., 2019; Bernardo et al., 2024; McNulty, 2023). When third-party intelligence and readiness services contribute to these artifacts in ways that strengthen traceability and governance defensibility, vendor relationships can enhance resilience and readiness. When vendor outputs are consumed without adequate internal validation or documentation of how they informed governance decisions, they risk complicating rather than clarifying the evidence base that examiners assess.

### *Synthesis and Identified Research Gaps*

The reviewed literature converges on three consistent conclusions that define the theoretical landscape of this study. First, regulatory readiness in large financial institutions is increasingly conceptualized and evaluated as a governance capability—dependent on accountable leadership, information artifact quality, documented decision traceability, and adaptive governance routines (BCBS, 2021; Caluwe et al., 2024; Abraham et al., 2019; Li et al., 2021). Second, CTI is empirically well-established as an operational enabler, but its contribution to governance defensibility and regulatory examination readiness remains theoretically underdeveloped and empirically underexamined, particularly for externally sourced, vendor-provided intelligence (Ainslie et al., 2023; Zibak et al., 2022; Wagner et al., 2019). Third, third-party vendor relationships introduce governance risks that are amplified in regulated environments, and the mechanisms through which vendor outputs are evaluated, validated, and

integrated into institutional governance processes represent a critical and understudied area of empirical inquiry (Oshri et al., 2019; BCBS, 2021; Li et al., 2021).

A primary and consequential research gap persists across all three themes: the empirical literature does not adequately explain how governance professionals within large, federally regulated financial institutions evaluate, validate, and operationalize third-party CTI within regulatory readiness processes. The result is an absence of outcome-based evidence that practitioners can use to make defensible decisions about vendor investment, internal capability development, and regulatory readiness strategy. A qualitative, single-case study focused on the evaluative processes, governance routines, and evidentiary practices of experienced cybersecurity governance professionals within a G-SIB institution is methodologically well-suited to address this gap.

## Chapter 3: Research Methodology

This chapter describes the study's methodological architecture, providing the scholarly justification, procedural details, and ethical framework required to assess its rigor and trustworthiness. The chapter is organized around the core methodological decisions that govern the study: the qualitative single-case design, the purposive sampling strategy, the semi-structured interview protocol, the thematic analysis procedure, and the safeguards employed to ensure credibility, dependability, confirmability, and transferability. Each decision is grounded in methodological literature and explained in relation to the study's research questions, the nature of the phenomenon under investigation, and the specific institutional context in which data will be collected. Taken together, these procedures constitute a coherent methodological strategy for generating rigorous, empirically grounded insight into a governance problem of considerable practical and scholarly consequence for large, regulated financial institutions.

The purpose of this qualitative single-case study is to explore how cybersecurity, risk, and compliance professionals within a large, U.S.-based, globally systemically important bank (G-SIB) evaluate the regulatory-readiness value of third-party cyber threat intelligence (CTI) and vendor-supported services. The participating institution is headquartered in New York. It is subject to consolidated supervision by the Federal Reserve Board, examination authority of the Office of the Comptroller of the Currency (OCC), and oversight by the Consumer Financial Protection Bureau (CFPB). The institution operates across more than 160 countries, employs one of the largest enterprise cybersecurity governance programs in the financial services industry, and is subject to annual supervisory examinations and stress testing requirements under the Dodd-Frank Wall Street Reform and Consumer Protection Act (2010). The organization is not named in this

study to preserve participant confidentiality and comply with the institution's data governance requirements.

The study does not seek to test hypotheses, establish statistical relationships, or generalize findings to a broader population. Its purpose is to develop a rich, contextualized, and empirically grounded understanding of how experienced governance professionals interpret, assess, and operationalize third-party CTI in response to the specific governance and regulatory demands of a G-SIB institution. This purpose is inherently suited to a qualitative approach, which enables the nuanced examination of complex evaluative processes and professional judgment that structured surveys or numerical instruments cannot adequately capture (Creswell & Creswell, 2023; Yin, 2018).

### *Role of the Researcher*

In qualitative inquiry, the researcher serves as the primary instrument for data collection and interpretation—a role that entails significant methodological responsibility (Creswell & Guetterman, 2019; Ravitch & Carl, 2021). For this study, the researcher will design the interview protocol, conduct all semi-structured interviews, manage data storage and anonymization procedures, and execute the thematic analysis of interview transcripts. The researcher brings professional experience in cybersecurity governance, regulatory compliance, and risk management within regulated institutional environments. This background facilitates the development of contextually informed interview questions and enables interpretively nuanced engagement with participant responses. It also introduces the potential for confirmatory bias. The researcher acknowledges this risk explicitly and employs the bracketing procedures described in the following section to mitigate its influence throughout the research process.

### *Researcher Bias and Bracketing*

Bracketing is a disciplined practice through which the researcher consciously identifies personal assumptions, prior experiences, and professional predispositions and deliberately sets them aside during data collection and analysis, allowing participant perspectives to drive the interpretive process (Creswell & Creswell, 2023; Tracy, 2020). Given the researcher's professional background in cybersecurity governance and vendor management, bracketing is particularly important to ensure that findings reflect participant perspectives rather than the researcher's own evaluative frameworks. Four procedural safeguards will support this process: a reflexive journal maintained throughout data collection and analysis to document assumptions and interpretive inclinations in real time; open-ended interview questions that invite participants to describe experiences in their own terms without presupposing conclusions; an inductive coding procedure in which initial codes are generated from transcript content before being organized into higher-order categories; and a documented analytical audit trail recording all interpretive decisions, supporting the confirmability of findings and enabling external review.

### *Overview of the Research Methodology*

This study employs a qualitative research methodology with a single-case study design. Qualitative research is appropriate when the investigative goal is to explore and interpret how individuals construct meaning, navigate complex processes, and exercise professional judgment within real-world organizational contexts (Creswell & Creswell, 2023; Miles et al., 2020). The study's research questions are oriented toward interpretive and evaluative processes: how cybersecurity governance professionals define and assess the regulatory-readiness value of external intelligence, how vendor outputs are operationalized through governance mechanisms, and what challenges arise in translating vendor intelligence into examination-ready evidence.

These questions demand an investigative method capable of capturing the complexity, context-dependence, and interpretive depth of professional governance experience—a demand that qualitative inquiry is designed to meet.

A case study design is appropriate because it enables in-depth examination of a contemporary phenomenon within its real-life institutional context (Hancock et al., 2021; Yin, 2018; Thomas, 2021). The participating institution constitutes a revelatory case (Yin, 2018): a site with characteristics—G-SIB designation, multi-regulatory oversight, global scale, and an extensive third-party vendor ecosystem—that make it an especially information-rich setting for examining the research questions. The single-case approach prioritizes depth of understanding within a bounded organizational context over breadth of coverage, consistent with the study's exploratory and explanatory ambitions.

## Discussion on the Population and Sampling

The target population for this study comprises cybersecurity, risk management, and compliance professionals at the participating G-SIB institution who have direct responsibility for cybersecurity regulatory readiness activities. Roles within this population include cybersecurity managers and directors, governance, risk, and compliance (GRC) professionals, technology risk officers, regulatory compliance specialists, information security leaders, and senior analysts with examination-preparation responsibilities. What unites this population is not a particular job title but a shared professional function: direct engagement with the governance processes, vendor relationships, and documentation practices through which the institution prepares for and responds to regulatory examinations. Qualitative research on complex professional phenomena is most informative when participants are selected for the depth of their relevant experience rather than

their representativeness of a broader statistical population (Creswell & Creswell, 2023; Miles et al., 2020), and the target population identified for this study meets that criterion.

### *Sampling Method*

A purposive sampling strategy will be employed to identify participants with professional experience and governance responsibilities most relevant to the study's research questions. Purposive sampling—also termed criterion-based or judgment sampling—is the dominant approach in qualitative case study research when the investigative goal is to select information-rich participants whose experiences can illuminate the phenomenon of interest rather than to achieve statistical representativeness (Ahmad & Wilkins, 2025; Creswell & Creswell, 2023). This strategy ensures that every participant has direct, substantive experience evaluating third-party CTI or vendor-supported regulatory-readiness services in the governance and examination-preparation context examined by the study.

### *Sample Size Determination*

The anticipated sample size is 15 to 18 participants, consistent with sample size guidance for qualitative single-case study research that prioritizes depth of insight and thematic richness (Hancock et al., 2021; Braun & Clarke, 2022). Rather than a predetermined fixed number, the final sample size will be guided by the principle of data saturation—the point at which additional interviews yield no meaningfully new codes, categories, or thematic patterns related to the research questions (Braun & Clarke, 2022; Miles et al., 2020). Because participants share similar governance responsibilities within a single institutional context, thematic saturation is expected to be achievable within the projected range.

### *Inclusion and Exclusion Criteria*

Participants must satisfy the following inclusion criteria: current employment within the participating G-SIB institution; professional responsibilities in cybersecurity governance, regulatory compliance, or risk management; direct involvement in regulatory readiness planning, examination preparation, or cybersecurity governance oversight; and substantive experience evaluating or interacting with third-party cybersecurity vendors or threat intelligence providers. Individuals who do not meet these criteria will be excluded from the study, as their professional experience would not provide the governance-relevant insights required by the research questions.

### *Sampling Challenges and Limitations*

Several practical challenges may affect the sampling process. Access to eligible participants within a large, regulated financial institution may be constrained by workload pressures, information sensitivity requirements, and institutional approval timelines. Voluntary participation may introduce self-selection effects: professionals who elect to participate may hold more differentiated views on the effectiveness of vendor intelligence than those who decline. Recruitment across multiple governance and compliance functions will partially mitigate this risk by encouraging participation from professionals with varied roles and perspectives.

## Data Collection and Data Analysis

### *Data Collection Methods*

Semi-structured interviews constitute the primary method of data collection for this study. Semi-structured interviews are well-suited to this investigation because they provide sufficient structure to ensure consistent coverage of topics most relevant to the research questions while allowing participants to elaborate and develop responses in their own terms (Hancock et al., 2021;

Trainor & Graue, 2022). This combination is particularly valuable in a study of complex professional judgment and governance practice, where the most analytically significant insights frequently emerge from participants' unprompted elaborations rather than from direct responses to predetermined questions. A limited documentary review may supplement interview data when relevant organizational artifacts—such as governance documentation, regulatory readiness reports, and vendor evaluation frameworks—are accessible and appropriate to review, given the institution's confidentiality requirements, thereby supporting the triangulation strategy described below.

### *Data Collection Instruments*

Two instruments will be used to structure and systematize data collection. The first is a ten-question participant eligibility screening survey designed to confirm that prospective participants meet the study's inclusion criteria and possess the professional experience to address the research questions substantively. The second is a semi-structured interview protocol comprising seven open-ended questions, with accompanying probes, exploring: the participant's role in cybersecurity regulatory readiness; how third-party CTI influences governance and examination preparation processes; the value participants perceive vendor-supported services to provide; the criteria through which vendor intelligence effectiveness is evaluated; challenges and limitations encountered; opportunities for improving intelligence integration; and perspectives on internally developed or AI-assisted alternatives to third-party services. The full protocol is reproduced in Appendix E.

### *Data Collection Procedures*

Following receipt of institutional approval and IRB authorization, eligible participants will be recruited through cybersecurity governance teams, compliance departments, and internal

professional networks within the participating institution. Prospective participants will complete the eligibility screening survey to verify that the inclusion criteria are met. Eligible participants will be contacted to schedule interviews conducted via a secure virtual meeting platform. Prior to each interview, participants will review and execute an informed consent form detailing the study's purpose, participation procedures, confidentiality protections, and the right to withdraw at any time without consequence. Interviews will follow the semi-structured protocol and are expected to last 30 to 45 minutes. With participant consent, interviews will be audio-recorded to support accurate verbatim transcription; recordings will be transcribed promptly and stored securely.

### *Data Storage and Confidentiality*

All interview recordings will be stored in encrypted digital storage accessible only to the researcher. Transcripts will be anonymized upon creation: participant names will be replaced with unique alphanumeric identifiers, and identifying references to specific roles, teams, or organizational units will be generalized or redacted. Recruitment contact information will be stored separately from interview data and destroyed upon completion of data collection. All research materials will be maintained on password-protected devices and stored in accordance with the data management requirements of California Intercontinental University and the participating institution.

### *Data Analysis Procedures*

Interview transcripts will be analyzed using thematic analysis, following the systematic six-phase procedure described by Braun and Clarke (2022): familiarization with the data, generation of initial codes, development of candidate themes, review and refinement of themes, definition and naming of final themes, and production of the analytical report. Thematic analysis is appropriate for this study because it provides a systematic and transparent method for

identifying, organizing, and interpreting patterns of meaning across qualitative data—patterns corresponding to the evaluative processes, governance routines, and professional judgments through which participants assess third-party CTI within regulatory readiness contexts (Braun & Clarke, 2022; Miles et al., 2020). Data will be organized and coded using NVivo qualitative data analysis software, supporting systematic transcript management, consistent code application, and iterative development of the thematic structure.

*Table 3.1. Coding Structure for Thematic Analysis*

| **Code** | **Description** | **Example Evidence** |
|---|---|---|
| Vendor Intelligence Value | Participant perceptions of the usefulness or relevance of third-party CTI. | Statements describing benefits of vendor intelligence for exam preparation. |
| Governance Integration | How intelligence outputs are incorporated into internal governance processes. | References to risk assessments, compliance documentation, or board reporting. |
| Regulatory Readiness Outcomes | Perceived impact of CTI on examination preparedness and assessment consistency. | Descriptions of improved documentation, audit readiness, or regulatory confidence. |
| Vendor Dependency Risk | Concerns about over-reliance on third-party providers. | Comments about reduced internal capability or unclear accountability. |
| Cost and Investment Justification | How organizations evaluate the financial value of CTI services. | Discussion of budgeting decisions or ROI uncertainty. |

*Note.* Developed by the researcher.

*Table 3.2. Research Question Alignment Matrix*

| Research Question | Data Source | Analysis Method |
|---|---|---|
| RQ1: How do cybersecurity and compliance professionals perceive the effectiveness of third-party CTI in supporting regulatory readiness? | Semi-structured interviews | Thematic analysis |
| RQ2: How do decision-makers describe the role of third-party vendors in influencing readiness planning, assessment consistency, and investment decisions? | Semi-structured interviews; governance documents | Thematic analysis; document review |
| RQ3: What challenges or limitations do participants identify when using third-party CTI for regulatory examination preparation? | Semi-structured interviews | Thematic analysis |

*Note.* Developed by the researcher.

### *Data Triangulation*

Triangulation will be employed to strengthen the credibility and internal consistency of the study's findings. While semi-structured interviews constitute the primary data source, relevant organizational documents—governance artifacts, regulatory readiness materials, vendor oversight documentation—will be reviewed where accessible and appropriate. Convergence between interview accounts and documentary evidence will strengthen confidence in thematic conclusions; divergences will prompt further analytical interrogation (Hancock et al., 2021; Yin, 2018).

### *Ensuring Research Quality and Rigor*

The trustworthiness of this study will be evaluated against the four criteria proposed by Lincoln and Guba (1985) and elaborated in subsequent methodological scholarship: credibility, dependability, confirmability, and transferability (Enworo, 2023; Tracy, 2020). Credibility will be strengthened through in-depth participant engagement, extended interview duration, and member-checking procedures where feasible. Dependability will be supported through consistent application of the interview protocol, systematic documentation of analytical decisions, and the use of NVivo to ensure procedural transparency. Confirmability will be enhanced through the reflexive journal, the analytical audit trail, and the bracketing procedures described above. Transferability will be addressed through detailed, contextually rich descriptions of the participating institution, participant characteristics, and the institutional environment, providing readers with sufficient information to assess whether the findings are analytically applicable to comparable organizational settings.

## Assumptions, Limitations, and Delimitations

### *Assumptions*

Three foundational assumptions underlie this study. First, the study assumes that participants possess the professional depth and institutional experience needed to provide substantive responses to the interview questions—an assumption supported by the eligibility screening procedure and purposive sampling strategy (Ahmad & Wilkins, 2025). Second, the study assumes that participants will respond with reasonable candor and accuracy; the confidentiality protections and anonymization procedures are designed to reduce social desirability effects and institutional sensitivity concerns that might otherwise constrain disclosure (Creswell & Guetterman, 2019). Third, the study assumes that governance practices within the participating

institution, while specific to its organizational context, share sufficient structural and regulatory similarities with comparable G-SIB institutions to support a meaningful assessment of transferability.

### *Limitations*

Several limitations constrain the study's scope and the applicability of its findings. The single-case design, while methodologically appropriate for the study's exploratory and explanatory purposes, limits generalizability to other institutional contexts. Self-selection bias in voluntary participation may produce a sample that over-represents professionals with particularly salient views about vendor intelligence. Confidentiality requirements may restrict the operational details that participants can disclose and the documentary evidence that they can access, thereby limiting the completeness of the triangulation strategy. These limitations are acknowledged transparently, and their implications are addressed through the methodological safeguards—purposive sampling, rigorous documentation, member checking, and transferability description—described throughout this chapter.

### *Delimitations*

The study is deliberately bounded in three respects. With respect to institutional scope, the study focuses exclusively on a single G-SIB institution; other financial institution types—regional banks, credit unions, investment advisers—are outside the study's scope because regulatory oversight frameworks, governance structures, and vendor ecosystems differ materially across institution types. Regarding participant scope, the study is limited to cybersecurity governance, risk management, and compliance professionals. Technical security operations staff, external regulators, and vendor representatives are excluded to maintain analytical focus on the governance decision-making processes through which regulatory readiness is constructed and evaluated. With

respect to methodological scope, the study employs a qualitative single-case design that privileges interpretive depth and contextual richness over statistical generalization—a deliberate choice grounded in the exploratory nature of the research questions and the current state of the empirical literature.

# CHAPTER 4: Results, Discussions, and Implications

This chapter presents the results of the qualitative single-case study examining how cybersecurity, risk, and compliance professionals within a large, U.S.-based, globally systemically important bank (G-SIB) evaluate the regulatory-readiness value of third-party cyber threat intelligence (CTI) and vendor-supported services. The chapter is organized to move from data collection and participant context, through thematic findings, to a discussion that situates those findings within the conceptual framework and literature introduced in Chapter 2. The chapter begins with a brief overview of the data collection process and participant characteristics, followed by a presentation of findings organized by theme and aligned to the study's three research questions. A discussion section then interprets these findings in relation to the conceptual framework and existing scholarship on cybersecurity governance, threat intelligence, and third-party risk management. The chapter concludes with implications for practice and theory, recommendations for future research, and a summary of the study's contributions.

## *Purpose of the Study*

The purpose of this qualitative single-case study was to explore how cybersecurity, risk, and compliance professionals within a large, U.S.-based G-SIB evaluate the regulatory-readiness value of third-party cyber threat intelligence and vendor-supported services. Financial institutions of this scale operate under intensifying cybersecurity regulatory scrutiny while continuing to invest substantial resources in external intelligence and advisory services intended to strengthen examination preparedness (Basel Committee on Banking Supervision [BCBS], 2021; National Institute of Standards and Technology [NIST], 2024). Despite this investment, limited empirical evidence exists regarding how organizational decision-makers determine whether vendor-supported intelligence meaningfully contributes to regulatory readiness

outcomes. This study addressed that evidentiary gap by examining how professionals with direct governance and examination responsibilities define effectiveness, justify investment decisions, and integrate vendor-provided intelligence into readiness planning within a single, information-rich institutional context (Yin, 2018).

### *Research Questions*

The study was guided by three research questions, each addressing a distinct dimension of the evidentiary gap identified in Chapter 1.

***RQ1:*** *How do cybersecurity and compliance professionals within a large, federally regulated U.S. financial institution perceive the effectiveness of third-party threat intelligence in supporting regulatory readiness?*

***RQ2:*** *How do decision-makers describe the role of third-party vendors in influencing regulatory readiness planning, assessment consistency, and investment decisions?*

***RQ3:*** *What challenges or limitations do participants identify when using third-party threat intelligence for regulatory examination preparation?*

Together, these questions directed the collection and analysis of data toward understanding not only whether third-party CTI and vendor-supported services are perceived as effective, but how that effectiveness is constructed, operationalized, and constrained within a regulated governance environment (Ainslie et al., 2023; Tallon et al., 2013). The findings presented in this chapter are organized to address each research question in turn, following the thematic analysis procedures described later (Braun & Clarke, 2022).

### *Overview of the Chapter*

The remainder of this chapter is organized into five sections. The first section summarizes the data collection process, including the instruments and procedures used,

participant characteristics, and the extent of data saturation achieved. The second section presents the study's findings organized by theme, drawing on participant interview data and triangulated screening-survey data. The third section aligns these thematic findings explicitly with RQ1, RQ2, and RQ3. The fourth section discusses the findings in relation to the conceptual framework and literature reviewed in Chapter 2. The chapter concludes with the implications of the findings for cybersecurity governance practice and theory, recommendations for future research, and a summary of the study's overall contribution.

The following sections describe the data collection and analysis methods used in this qualitative single-case study, including the tools used to administer instruments, capture data, and support analysis, as well as the safeguards used to strengthen the validity and reliability of the findings.

### *Data Collection Methods and Instruments*

Consistent with Chapter 3, two instruments guided data collection. A ten-question eligibility screening survey confirmed that prospective participants held cybersecurity governance, compliance, or risk management roles involving direct experience with third-party CTI or vendor-supported readiness services. Eligible participants then completed a semi-structured interview comprising seven open-ended questions and probes addressing participants' governance roles, their perceptions of vendor-supported intelligence, the criteria used to evaluate its effectiveness, and related integration challenges. Interviews lasted approximately 30 to 45 minutes, consistent with the protocol reproduced in Appendix E.

### *Tools and Software*

Three platforms supported data collection and analysis. Qualtrics XM was used to build and distribute the screening survey, collect responses, and generate descriptive summaries that

informed purposive sampling decisions. Microsoft Teams and Zoom were used to conduct interviews and capture the corresponding verbatim transcripts, which were reviewed against each session's recording for accuracy prior to analysis. Transcripts and survey exports were then organized and coded in NVivo, which supported systematic transcript management, consistent code application, and iterative development of the thematic structure, in line with Braun and Clarke's (2022) six-phase procedure.

### *Data Analysis Procedures*

Interview transcripts served as the primary data source. They were analyzed using thematic analysis, following Braun and Clarke's (2022) six-phase procedure: familiarization, initial coding, candidate theme development, theme review and refinement, theme definition and naming, and production of the analytical report. Qualtrics XM survey data provided contextual and demographic information used to characterize the sample and support triangulation across sources, consistent with the case study approach described by Yin (2018) and Hancock et al. (2021).

### *Validity and Reliability*

Trustworthiness was evaluated against the four criteria proposed by Lincoln and Guba (1985): credibility, dependability, confirmability, and transferability (Enworo, 2023). Credibility was supported through extended participant engagement and verbatim, platform-generated transcripts cross-checked against session recordings, ensuring the analyzed data reflected participants' own words rather than summarized content. Dependability was supported by the consistent application of the interview protocol and the systematic documentation of coding decisions in NVivo. Confirmability was strengthened through a reflexive journal maintained throughout data collection and analysis, as well as a documented analytical audit trail of

interpretive decisions. Transferability was addressed through a detailed contextual description of the participating institution and participant characteristics, allowing readers to assess whether findings may be analytically, rather than statistically, applicable to comparable settings (Yin, 2018). Together, these tools and procedures produced a systematically collected and analyzed dataset supporting the rigor of the findings presented in the remainder of this chapter.

### *Participant Characteristics and Data Saturation*

The screening survey yielded 42 respondent records, of which 39 completed the full nine-item instrument beyond the consent gate; three respondents exited immediately after consenting and provided no further data. Consistent with the purposive, criterion-based sampling strategy described in Chapter 3, I used respondents' answers regarding regulatory-examination involvement, use of third-party CTI, and willingness to be interviewed to identify candidates for the semi-structured interview phase (Hancock et al., 2021). Twenty-five of the 39 respondents (64.1%) indicated willingness to participate in a follow-up interview, and 18 of those individuals completed a full semi-structured interview and produced a usable, platform-generated verbatim transcript. This yield sits within the 15-to-18-participant range established as the study's purposive sampling target and is consistent with sample sizes reported in comparable single-case qualitative studies of specialized organizational populations (Hancock et al., 2021; Yin, 2018).

To further protect participant confidentiality beyond the recruitment-tracking numbers used during data collection, I assigned each of the 18 interviewed individuals a sequential analytic identifier, P01 through P18, corresponding to the chronological order in which their original recruitment number appears in the interview log. These identifiers, rather than the original recruitment numbers, are used throughout the remainder of this chapter to reference

participant data. Table 4.1 summarizes the characteristics of the analytic sample, drawing on the demographic and role-based fields captured during the initial screening survey.

The analytic sample was weighted toward senior and experienced practitioners: 15 of the 18 participants (83.3%) reported more than 10 years of professional experience in cybersecurity, risk management, or regulatory compliance, 7 (38.9%) held senior-leadership-level roles, and a further 9 (50.0%) held manager- or team-lead-level roles. Governance, risk, and compliance (GRC); cybersecurity operations, including offensive security and red-team functions; regulatory compliance; risk management; and executive cybersecurity leadership were the functional areas most frequently represented, reflecting the study's purposive emphasis on recruiting participants positioned at the intersection of cybersecurity operations and regulatory governance (BCBS, 2021; NIST, 2024). The extent of responsibility for evaluating or interpreting vendor-supplied intelligence varied meaningfully across the sample: 10 participants (55.6%) described limited responsibility in this area, 7 (38.9%) described moderate responsibility, and 1 (5.6%) described significant, first-line responsibility for evaluating vendor intelligence. This distribution proved analytically useful because it allowed the coding process to capture the perspective of both direct evaluators of vendor intelligence and downstream consumers of vendor-informed outputs. This distinction became central to Theme 3 below.

**Table 4.1**

*Participant Characteristics (N = 18)*

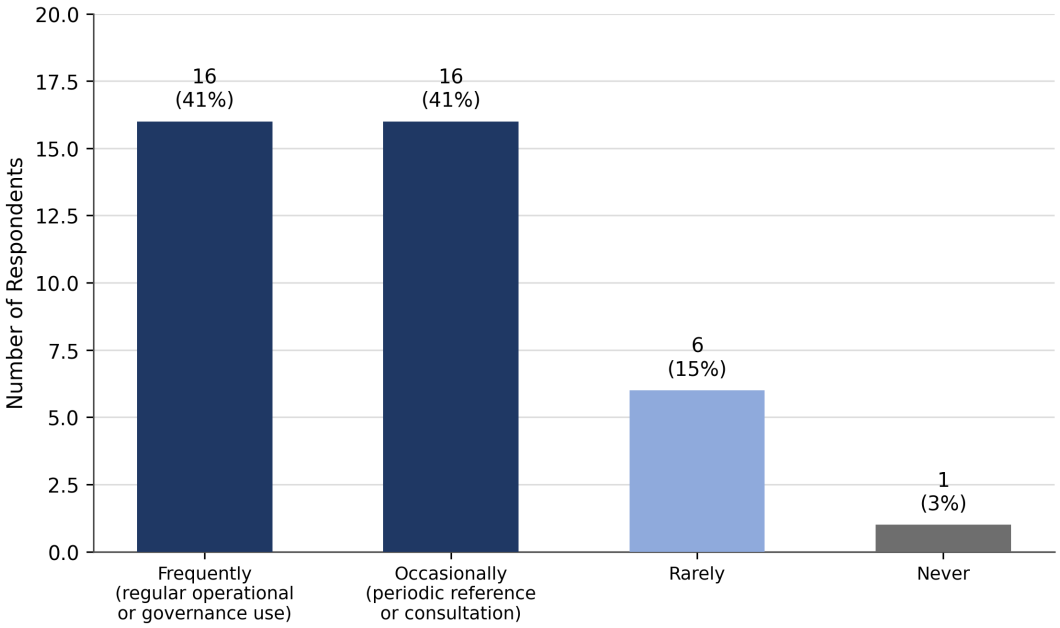
| Participant ID | Seniority Level | Primary Functional Area(s) | Years of Experience | Frequency of Vendor Reliance | Extent of Vendor-Evaluation Responsibility |
|---|---|---|---|---|---|
| P01 | Senior Leadership | IT Security Architecture / Engineering | More than 10 years | Occasionally | Limited |
| P02 | Manager / Team Lead | Risk Management; Executive Cybersecurity Leadership; Other | More than 10 years | Frequently | Limited |
| P03 | Senior Leadership | Executive Cybersecurity Leadership | More than 10 years | Occasionally | Moderate |
| P04 | Manager / Team Lead | Other | More than 10 years | Occasionally | Limited |
| P05 | Manager / Team Lead | Cybersecurity Operations; GRC; Regulatory Compliance; Risk Mgmt.; Internal Audit; IT Sec. Arch.; Other | Less than 3 years | Frequently | Moderate |
| P06 | Manager / Team Lead | Regulatory Compliance | More than 10 years | Occasionally | Limited |
| P07 | Manager / Team Lead | Offensive Security | More than 10 years | Frequently | Moderate |
| P08 | Manager / Team Lead | Cybersecurity Operations | More than 10 years | Occasionally | Moderate |
| P09 | Senior Leadership | Governance, Risk, and Compliance (GRC) | 3–5 years | Rarely | Limited |
| P10 | Senior Leadership | GRC; Regulatory Compliance; Risk Mgmt.; Internal Audit | More than 10 years | Occasionally | Limited |

| Participant ID | Seniority Level | Primary Functional Area(s) | Years of Experience | Frequency of Vendor Reliance | Extent of Vendor-Evaluation Responsibility |
|---|---|---|---|---|---|
| P11 | Senior Leadership | GRC; Cybersecurity Operations; Risk Mgmt.; Regulatory Compliance | More than 10 years | Occasionally | Limited |
| P12 | Senior Leadership | Executive Cybersecurity Leadership | More than 10 years | Frequently | Moderate |
| P13 | Senior Leadership | Risk Management | More than 10 years | Frequently | Limited |
| P14 | Manager / Team Lead | GRC; Regulatory Compliance; IT Sec. Arch.; Other | More than 10 years | Occasionally | Moderate |
| P15 | Manager / Team Lead | Cybersecurity Operations | More than 10 years | Occasionally | Moderate |
| P16 | Individual Contributor | GRC; Regulatory Compliance | More than 10 years | Frequently | Significant |
| P17 | Individual Contributor | IT Security Architecture / Engineering | 3–5 years | Occasionally | Limited |
| P18 | Manager / Team Lead | GRC; Regulatory Compliance; Risk Mgmt.; Executive Cybersecurity Leadership | More than 10 years | Frequently | Limited |

*Note.* Developed by the researcher. Seniority level, functional area, years of experience, frequency of vendor reliance, and extent of vendor-evaluation responsibility were captured through the Qualtrics XM screening survey (Chapter 3, Appendix D) and are reported here using the anonymized analytic identifier assigned to each interviewed participant. GRC = Governance, Risk, and Compliance.

**Figure 4.1**

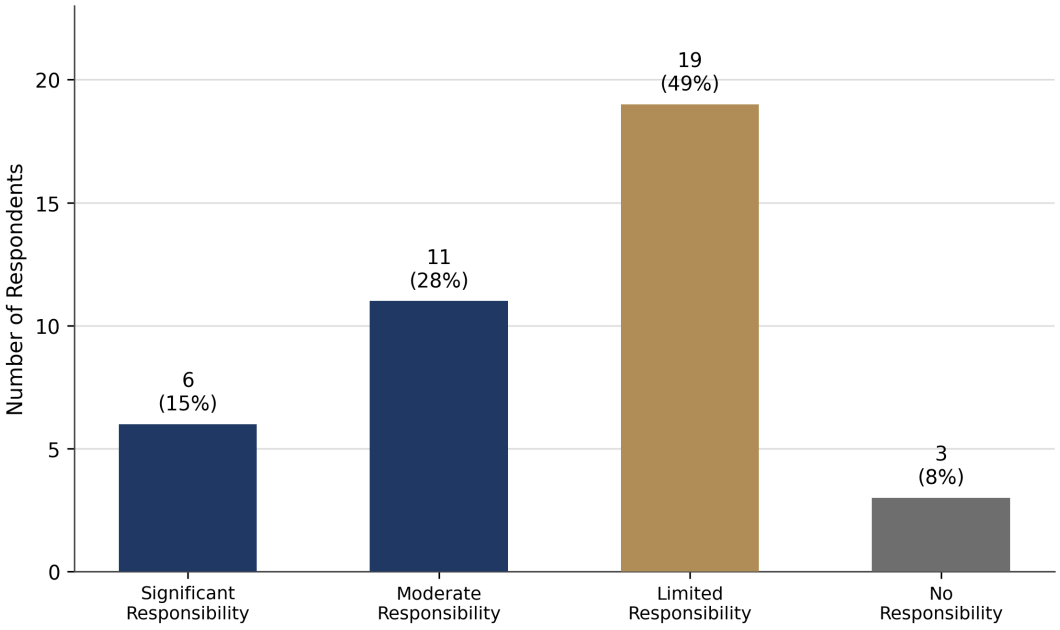
*Screening-Survey Frequency of Reliance on Vendor-Provided Threat Intelligence or Advisory Services (N = 39)*




*Note.* Developed by the researcher. The data reflect all 39 respondents who completed the screening survey item beyond the consent gate, not only the 18 interviewed participants. Percentages are rounded to the nearest whole number.

**Figure 4.2**

*Screening-Survey Extent of Responsibility Evaluating or Interpreting Vendor-Supplied Intelligence (N = 39)*




*Note.* Developed by the researcher. The data reflect all 39 respondents who completed the screening survey item beyond the consent gate, not only the 18 interviewed participants. Percentages are rounded to the nearest whole number.

I assessed data saturation using the constant-comparison approach embedded in Braun and Clarke's (2022) six-phase thematic analysis procedure, tracking in NVivo whether each successive interview transcript generated codes not already represented in the developing codebook (Chapter 3, Tables 3.1 and 3.2). Codes stabilized progressively across the interview sequence: the final four interviews each produced fewer than two new open codes, and none of the six themes reported below emerged for the first time after the fourteenth interview. Rather, these later interviews served primarily to confirm, deepen, or add contextual nuance to the existing thematic structure, a pattern consistent with the redundancy-based approach to case-based data adequacy described by Hancock et al. (2021). I treat this pattern as evidence that the

18-participant sample achieved sufficient depth for the analytic, rather than statistical, generalization appropriate to a single-case design (Yin, 2018).

### *Presentation of Findings by Theme*

Applying Braun and Clarke's (2022) six-phase thematic analysis procedure—familiarization, systematic coding, candidate theme generation, theme review, theme definition and naming, and production of the analytic narrative—to the 18 verbatim interview transcripts, I identified six interrelated themes. Table 4.2 summarizes each theme's definition, illustrative codes, and primary alignment to the study's research questions. Figure 4.3 displays the number of participants whose transcripts contributed coded data to each theme, offering a triangulation check on thematic prevalence across the sample. The themes are presented in the order that best reflects the logical flow of the findings—from the conditions under which participants perceived third-party intelligence as effective, through the criteria and constraints that shaped its integration, to the persistent data-quality challenges and the emerging role of artificial intelligence—rather than strictly in order of prevalence. Consistent with the case study protocol described in Chapter 3, I supplement each theme with corroborating evidence from the Qualtrics screening survey dataset (N = 39), where relevant, thereby providing methodological triangulation across data sources (Hancock et al., 2021; Yin, 2018). Direct quotations are reproduced from platform-generated, recording-verified transcripts, lightly edited only to remove verbal disfluencies (e.g., false starts, filler words) without altering substantive meaning, and are attributed by analytic participant identifier (P01–P18) only; no identifying organizational, vendor, or personal information is reproduced.

**Table 4.2**

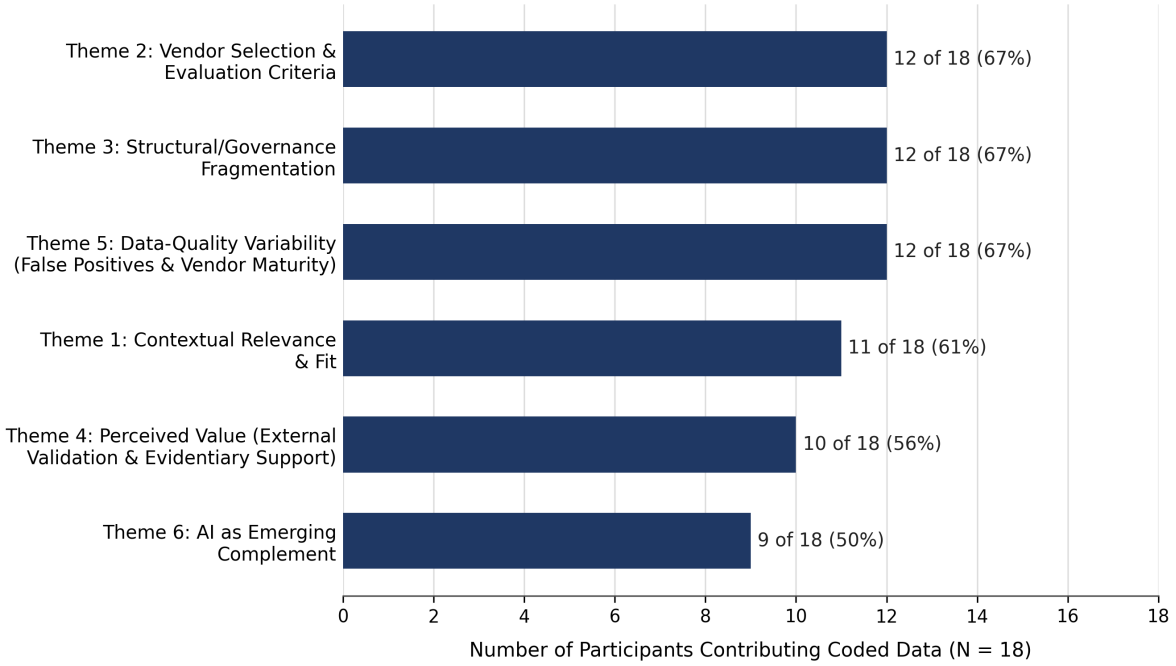
*Thematic Structure Overview*

| Theme | Definition | Illustrative Codes | Primary Research Question Alignment |
|---|---|---|---|
| 1. Contextual Relevance and Fit | Perceived effectiveness tracks how precisely vendor intelligence reflects firm-specific business lines, geography, and risk exposure | generic vs. tailored intel; global–local gap; scenario customization | RQ1 |
| 2. Vendor Selection and Evaluation Criteria | Formal and informal criteria organizations use to select and evaluate CTI and readiness vendors | regulator-approved vendor lists; referral/reputation; statement-of-work compliance | RQ2 |
| 3. Structural and Governance Fragmentation | Organizational and systems-level fragmentation limiting integration of vendor intelligence | first-/second-line silos; disconnected systems; onboarding lag; global–local governance mismatch | RQ2, RQ3 |
| 4. Perceived Value: External Validation, Access, and Evidentiary Support | Positive value drivers participants associated with vendor intelligence | unbiased perspective; talent/scale access; evidentiary documentation | RQ1 |
| 5. Data-Quality Variability | Persistent quality problems in vendor output | false positives; inconsistent scoring; vendor maturity/staffing variance | RQ3 |
| 6. AI as an Emerging Complement | AI's growing but human-supervised role in readiness work | control-mapping automation; response drafting; human-in-the-loop caution | RQ1, RQ3 |

*Note.* Developed by the researcher. Codes were developed and applied in NVivo following Braun and Clarke's (2022) six-phase procedure and are consistent with the codebook structure established in Chapter 3 (Tables 3.1 and 3.2).

**Figure 4.3**

*Thematic Prevalence Across the Interview Sample*




*Note.* Developed by the researcher. Counts reflect the number of the 18 interviewed participants (P01–P18) whose transcripts contributed at least one coded excerpt to the theme. Themes are not mutually exclusive; most transcripts contributed coded data to more than one theme.

### *Theme 1: Contextual Relevance and Fit as the Central Determinant of Perceived Effectiveness*

Across 11 of the 18 interviews (61.1%), participants found the effectiveness of third-party CTI not in the presence or absence of vendor intelligence itself, but in the extent to which that intelligence reflected the organization's specific business lines, geography, technology stack, and risk exposure. Generic or broadly scoped intelligence was repeatedly described as of marginal practical value. In contrast, intelligence that had been customized, or that participants had actively worked to customize, was described as materially more useful.

This pattern was most pronounced among participants in offensive-security and red-team-adjacent roles. P07, describing the limitations of vendor threat feeds at enterprise scale, explained:

> In many cases, the threat intel presented to us will be very, very generic. Moreover, if they try to dive deeper into it, it usually misses the point or the actual risk itself, either due to… the business changing, the… mergers and acquisitions the firm has undergone in recent years, the restructuring, or even legacy systems being phased out. (P07)

P07 further distinguished between broad, well-covered threats and the organization-specific detail regulators and internal stakeholders need, observing that vendors "do get it right for very high-profile threat actors" but that "what they do not do well is trying to contextualize it to us." This distinction between broad threat-landscape awareness and organization-specific applicability recurred among participants operating in international or regional roles. P06, a cybersecurity lead for an international operating region, described a persistent gap between globally produced intelligence and the information a regional governance body needed, estimating that a board briefing built solely from centrally distributed threat intelligence would represent only "about 15% of what is out there" for that jurisdiction.

Contextual fit was not framed solely as a limitation; several participants described active practices to increase it. P02 contrasted generic messaging with intelligence-based scenario design grounded in real precedent, explaining that instead of a vague warning that "any hacker could hack you and destroy your systems," an effective engagement uses "an actual scenario based on intelligence on something that already happened in the wild," which the organization then tailors to its own environment. Similarly, P15 described collaborative scoping between the organization and the vendor as the mechanism that converts generic threat-actor intelligence into a defensible test plan, stating that "collaborative effort in the planning phases is critical because it gives them a more successful plan." P08 offered a related but more cautionary observation, noting that vendor intelligence "may also place too much emphasis on geographic or industry targeting

without adequately contextualizing those threats to the organization specifically," which can shift the perceived risk landscape without necessarily improving its accuracy.

Taken together, these accounts indicate that participants evaluate third-party CTI effectiveness on a contextual-fit continuum rather than as a binary property of using, or not using, a vendor. This finding directly informs RQ1 and is further developed in the section that aligns the findings with the research questions.

### *Theme 2: Vendor Selection and Evaluation Criteria*

Twelve of the 18 participants (66.7%) described concrete criteria used to select or evaluate third-party CTI and readiness vendors, which clustered into three related but distinct patterns: regulator-mandated accreditation, informal reputational vetting, and contractual or statement-of-work (SOW) compliance.

The most consequential pattern, in terms of constraining vendor choice, was regulator-driven accreditation. P15 described how the choice of threat-intelligence provider is frequently dictated by the specific regulatory exercise rather than by open-market evaluation:

> It does depend a little bit on the regulatory exam… certain ones, for example, I think CBEST is one and TIBER, where they will only take TI, so threat intel, from specific vendors, or vendors that they prefer. So you kind of have to be conscientious of what you're running. (P15)

This account is consistent with the formal accreditation requirements documented in the Bank of England's CBEST threat-intelligence-led assessment framework and the European Central Bank's TIBER-EU framework, both of which require threat-intelligence and red-team providers to hold specific jurisdictional accreditation before their output can be used in a regulator-recognized exercise (Bank of England, 2024; European Central Bank, 2018). P08

described an analogous, if less formal, pattern, noting that regulator guidance—citing the Monetary Authority of Singapore's threat-intelligence reporting expectations as an example—establishes “a good foundation of what the provider should minimally provide” (Monetary Authority of Singapore, 2021), which the organization then uses as an evaluation baseline independent of a vendor's own marketing claims.

Where regulatory accreditation did not dictate vendor choice outright, participants described relying on informal reputational signals. P01 described word-of-mouth referral as a primary evaluation mechanism, explaining that the CTI vendor market is smaller than it appears and that talking “to someone who has used that vendor before” carries significant weight in selection decisions, alongside a regulator-imposed rotation requirement that periodically forces the organization to bring in a new provider, regardless of whether they are good or not. P14 described a more elaborate reputational due diligence process, screening vendors on their contributions to open-source security tooling, published thought leadership, and participation in peer-reviewed or trade-association venues as a proxy for technical credibility, explaining that when a vendor is “regularly writing about” evolving standards, “those go a long way” toward the organization's trust in that vendor's judgment.

Finally, several participants described contractual mechanisms as the operative evaluation criterion once a vendor was engaged. P09 described the statement of work as the functional standard against which vendor performance is judged. When a vendor “meets that statement of work and… checks off all the boxes of what we are requiring before they send us a report, that is how we are ensuring… the job has been completed fully.” This finding indicates that, for a substantial portion of the sample, vendor evaluation is procedural and compliance-oriented rather than an independent assessment of the quality of intelligence. This pattern connects directly to

Theme 5 below and bears on RQ2's focus on how vendors influence investment and assessment-consistency decisions.

### *Theme 3: Structural and Governance Fragmentation Limiting Integration*

Twelve participants (66.7%) described organizational or systems-level fragmentation that constrained how effectively third-party intelligence could be operationalized, independent of the intelligence's substantive quality. Three recurring sub-patterns emerged: information silos between first- and second-line functions, disconnected data systems, and a mismatch between globally produced intelligence and regionally governed decision-making.

The clearest articulation of a first-line/second-line information silo came from P13, whose second-line oversight role depends on visibility into intelligence that the first-line CISO organization does not consistently share:

> In Second Line, we have all… experienced a knowledge gap, and that is because First Line, um, the CISO organization, holds their information very tightly. So Second Line, which has performed the oversight, has limited intelligence and has to turn to open-source intelligence, which then hinders our ability to perform our function. (P13)

P10 described a related but structurally distinct governance gap, noting that the function responsible for regulatory coordination governs the internal teams that consume third-party intelligence but does not govern the intelligence itself: “I do not believe we govern third-party threat intelligence, because we only… govern [the team] who… consumes a lot of third-party threat intelligence, but we do not necessarily govern the intelligence that they are provided.” Taken together, these accounts suggest that oversight of vendor-supplied intelligence is unevenly distributed across governance layers, leaving no single function fully accountable for its quality.

A second sub-pattern concerned fragmented data systems. P15 described threat-intelligence output, exercise reporting, and control-gap findings as living in disconnected repositories—variously "in Excel files or PDFs or multiple things in various areas"—which made it difficult to track recurring themes across successive regulatory exercises or to distinguish a tactical, one-off finding from a strategic, recurring control gap. A related operational constraint was vendor onboarding lead time: P09 described a standard onboarding cycle of nine to twelve months, colliding with compressed regulatory timelines, observing that when a sponsor requested onboarding within 60 days, "it is not possible. It is literally not possible."

The third sub-pattern, evident specifically among internationally positioned participants, was a structural mismatch between centrally produced, U.S.-centered threat intelligence and the needs of regional governance bodies. P06 described this gap directly, noting that intelligence reporting is generated from a primarily domestic vantage point rather than being tailored to what each operating country's governance body needs to know, resulting in what the participant characterized as an incomplete picture for non-U.S. governance stakeholders despite the organization's substantial global footprint.

These findings indicate that structural and governance fragmentation—rather than the intrinsic quality of vendor intelligence—frequently determines whether relevant intelligence reaches the stakeholders who need it. This theme bears most directly on RQ2 and RQ3.

### *Theme 4: Perceived Value—External Validation, Specialized Access, and Evidentiary Support*

Ten participants (55.6%) articulated a clear positive value proposition for third-party CTI, and their accounts converged on three related sub-patterns: an external, unbiased perspective that internal teams cannot fully replicate; access to specialized talent and cross-sector visibility beyond what the organization could economically maintain internally; and evidentiary

or documentation value that is distinct from, and in some accounts more salient than, substantive readiness improvement.

Several participants in red-team and adversarial-emulation roles emphasized that internal familiarity with the organization's environment is itself a limitation that external vendors lack. P16 explained that an internal red team "know[s] they have a lot of insider information… they could potentially know how to get around certain things." In contrast, third-party testers "do not have that because they are completely unfamiliar with our network," which participants described as producing a more realistic simulation of an actual external attacker.

A second, related value driver was access to talent and cross-sector visibility that participants judged difficult or uneconomical to build internally. P08 described third-party vendors as providing "access to skilled professionals that smaller firms may not have the budget to hire, train, and retain," while also enabling attack simulation "without the bias of internal knowledge." P10 offered a forward-looking variant of this value proposition, describing vendor intelligence on artificial-intelligence-enabled attack methods as having positioned the organization ahead of regulator questioning:

> Every single audit we have had this year has asked, like, "What is your preparedness for an AI-induced cyberattack?" And I think our third-party vendors providing intelligence on that [] so that we were prepared in time to be informed and respond… has been tremendously helpful for regulatory requests and… coordination. (P10)

The third sub-pattern—evidentiary or documentation value—was articulated most directly by participants whose roles are closer to audit and examination logistics than to technical evaluation. P09 distinguished sharply between substantive preparation value and evidentiary value, explaining that a third party is "not really having a value in preparation per se, but the

value is in that we have the required evidence" to demonstrate due diligence to examiners. P12 extended this distinction into an explicitly skeptical register, characterizing the substantive value of vendor-provided threat intelligence as "little to none, with the exception of the presence of the [vendor] and the operational process of bringing the intel in," which nonetheless satisfies specific regulatory evidentiary requirements even where the participant did not believe the intelligence itself materially improved the organization's security posture.

This bifurcation between evidentiary value and substantive readiness value is analytically important: it indicates that "effectiveness," as participants use the term, is not a single construct but at minimum two distinct constructs—compliance-documentation sufficiency and security-posture improvement—that do not always move together. This finding is central to RQ1.

***Theme 5: Data-Quality Variability—False Positives and Uneven Vendor Maturity***

Twelve participants (66.7%) described data-quality problems as a persistent and, in several cases, operationally costly limitation of third-party CTI. Two closely related sub-patterns emerged: false positives that consume analyst time and erode trust in vendor output, and substantial variability in vendor maturity and staffing quality that participants had to manage actively.

False positives were described in vivid, operationally grounded terms. P05, a security engineer with direct security-operations-facing responsibility, identified false positives as the primary challenge with vendor-supported services, explaining that "a false positive, especially in the middle of the night, can be like one of the worst things for our team." P03 described a more structural version of the same problem, characterizing the relationship between vendor questionnaire responses and vendor-tool findings as requiring active reconciliation:

> It's a two-way [street] because we are using data that we require vendors to attest to. And then we are using… these tools to validate that information, but there's really a synergy there… You could have a great response and a poor outcome from the tool. Moreover, in that case, I want to talk to the vendor to understand where the gap is. Were they lying to me? (P03)

A related but distinct concern was inconsistency in vendor-reported risk-scoring data reaching parties outside the organization's control. P12 described a specific incident in which a prospective business contact produced a third-party security-rating report containing inaccurate attributions, requiring the participant to correct the record directly, and connected this experience to a broader call for standardization, observing that report quality varies by vendor in a pattern comparable to inconsistent software release notes—"the same mechanism, but the quality of the data is very different"—concluding that "the data quality would be an issue" even where standardized reporting formats exist.

The second sub-pattern, uneven vendor maturity and staffing, was described by participants across both governance and operational roles. P01 recounted repeated engagements staffed with junior consultants who required active supervision rather than delivering independent value, explaining, "I felt like we were teaching them what to do when they were supposed to come in and… be able to handle the work." P11 generalized this pattern across the vendor landscape, observing that "no two vendors are the same," and that smaller or less-resourced vendors, while capable, are "limited by their own size and scale," which measurably affects "the quality and robustness of what we receive from them."

These findings indicate that vendor-attributable data-quality variability, rather than a uniform baseline of vendor competence, is a primary driver of the skepticism evident in several participants' accounts, and this theme directly addresses RQ3.

### *Theme 6: Artificial Intelligence as an Emerging Complement, Not a Replacement*

Nine participants (50.0%) described active or planned use of artificial intelligence in support of regulatory-readiness work. Their accounts converged on a consistent position: AI was described as a productivity and pattern-detection multiplier for tasks that were previously manual and time-intensive, but participants uniformly qualified this value with explicit caution about submitting unverified AI output into a regulatory pipeline, positioning AI as a complement to, rather than a substitute for, human expert judgment and, in most accounts, for third-party vendor relationships.

The most concrete efficiency gains were described in control-framework mapping and regulatory-response drafting. P18 quantified a specific productivity gain from using a structured AI prompt to map existing internal controls against a standard framework:

> It is a manual exercise, probably taking a couple of people two or three weeks full-time… versus it took me about a week to do it with a sophisticated prompt. And I… validated the prompt and audited the prompt to ensure that it was not hallucinating that badly. You know, it was about 98% accurate based on my QA. (P18)

P10 described a comparable application at the point of regulatory-response drafting, explaining that an internally built tool that searches years of managing-director-approved prior responses converts what previously took weeks of subject-matter-expert coordination into a single query that a managing director then reviews and confirms remains current—collapsing what the participant described as a “never-ending infinity loop” of stakeholder coordination into

a substantially faster, though still human-reviewed, process. P01 described a third application pattern: using AI-driven behavioral anomaly detection on identity-access logs to flag likely account compromise and free security engineers from routine monitoring, allowing them to focus on higher-value project work.

Despite these efficiency gains, participants were emphatic that AI output required human validation before entering any regulator-facing artifact. P07 articulated this caution most directly, warning against submitting AI-generated material to a regulator without subject-matter-expert review because doing so risks producing "a professional-sounding report that does not hold up under scrutiny." P12 connected this caution to a recent, widely discussed industry incident involving unvalidated AI-generated compliance work product, stating that "it should be human assessed. Human oversight potentially can do this, but there can be scale problems," and cautioning that organizations must "really think through your architecture and the types of agents you're deploying and how you're supervising them."

Notably, one participant offered a counterpoint that reframes the relationship between AI and third-party vendors rather than treating them as substitutes: P08 explained that the organization deliberately continues to rely on third-party intelligence providers for regulation-driven engagements specifically because doing so yields intelligence "that is not overly biased or influenced by internal technologies or stakeholders," suggesting that, for at least some participants, external vendor intelligence and internal AI serve complementary rather than competing roles in the readiness process. Collectively, this theme informs both RQ1 (effectiveness is evolving alongside AI-augmented practice) and RQ3 (AI introduces a new category of oversight-related limitation).

### *Findings in Relation to the Research Questions*

The following section interprets the six themes presented above in direct relation to the study's three research questions, consistent with the interpretive requirement of a single-case design (Yin, 2018).

### *Research Question 1*

RQ1 asked how cybersecurity and compliance professionals within a large, federally regulated U.S. financial institution perceive the effectiveness of third-party threat intelligence in supporting regulatory readiness. The findings indicate that participants do not perceive effectiveness as a fixed or uniform property of using a third-party vendor. Instead, effectiveness is conditional and multidimensional, shaped jointly by Theme 1 (contextual relevance and fit), Theme 4 (the specific type of value delivered—external validation, specialized access, or evidentiary support), and Theme 5 (the data-quality variability that participants must actively manage). Several participants drew an explicit distinction between evidentiary sufficiency—having documentation that satisfies a specific regulatory requirement—and substantive improvement in the organization's actual security posture, and these two constructs did not always move together in participants' accounts. Theme 6 further indicates that the effectiveness construct itself is in motion: participants increasingly evaluate vendor intelligence alongside, and sometimes in intentional preference to, AI-augmented internal capability, and several explicitly cited AI-related threat scenarios as an area where vendor intelligence provided anticipatory value ahead of regulator inquiry. Overall, RQ1 findings support a contingent model of perceived effectiveness in which vendor intelligence is judged useful to the extent that it is organization-specific, independently corroborated, and clearly tied to a defined regulatory or operational outcome.

### *Research Question 2*

RQ2 asked how decision-makers describe the role of third-party vendors in influencing regulatory readiness planning, assessment consistency, and investment decisions. Findings organized under Theme 2 (vendor selection and evaluation criteria) indicate that vendor influence on planning and investment decisions is exercised less through open competitive evaluation of intelligence quality and more through structural channels: regulator-approved vendor and accreditation lists (e.g., CBEST- and TIBER-recognized providers; Bank of England, 2024; European Central Bank, 2018), informal reputational referral networks, and contractual statement-of-work compliance. This pattern suggests that, for a substantial share of participants, the vendor market that matters most operationally is defined by regulatory recognition rather than by independent efficacy testing. Assessment consistency, in turn, is constrained less by vendor quality than by the structural and governance fragmentation documented in Theme 3: information silos between first- and second-line functions, disconnected reporting systems, and a persistent mismatch between centrally produced and regionally relevant intelligence mean that the same vendor-supplied intelligence can be integrated thoroughly in one part of the organization and remain largely invisible in another. Collectively, these findings indicate that vendors substantially influence readiness activities but do so within and are constrained by organizational structures that participants themselves identified as needing improvement.

### *Research Question 3*

RQ3 asked what challenges or limitations participants identify when using third-party threat intelligence for regulatory examination preparation. Three limitations recurred with sufficient consistency to be treated as the study's principal answer to RQ3. First, generic or insufficiently contextualized intelligence (Theme 1) was the most frequently cited substantive

limitation, particularly among participants operating at enterprise scale or across multiple jurisdictions. Second, structural and governance fragmentation (Theme 3)—rather than vendor quality per se—limited the practical reach of even well-produced intelligence, with onboarding lead times, information silos, and disconnected data systems repeatedly cited as constraints independent of any single vendor's performance. Third, data-quality variability (Theme 5), particularly false positives and inconsistent vendor staffing and maturity, imposed a recurring validation burden on participants, which several described as lost analyst time and eroded trust. Emerging alongside these three established limitations, Theme 6 identifies a fourth, prospective limitation specific to this study's timing: the risk of unvalidated AI-generated content entering the regulatory-readiness pipeline without adequate human oversight, a concern participants raised proactively rather than in response to a direct interview prompt about AI risk. Taken together, these findings suggest that the limitations of third-party CTI are only partly attributable to vendors themselves; a substantial share is organizational and structural in origin and is, in principle, addressable independent of vendor selection.

### *Discussion of Findings*

This section extends the presentation of findings above by offering a detailed interpretation and discussion of the thematic analysis's findings on how cybersecurity, risk, and compliance professionals within this G-SIB evaluate the regulatory-readiness value of third-party cyber threat intelligence (CTI) and vendor-supported services. Where the preceding sections organized the six emergent themes and linked each individually to the study's three research questions, this discussion steps back to interpret those findings against five additional reference points central to the study's design: the research questions taken as a set, the conceptual framework introduced in Chapter 2, the themes anticipated before data collection, the applied

business problem that motivated the study, and the existing literature on cybersecurity governance, threat intelligence, and third-party risk management. Consistent with the interpretive expectations of a qualitative single-case design, this discussion privileges analytical generalization over statistical generalization and situates the findings within, rather than beyond, the bounded organizational context from which they were drawn (Yin, 2018).

### *The Research Questions*

Three research questions guided the study, each targeting a distinct facet of the evidentiary gap identified in Chapter 1: whether, how, and under what constraints third-party CTI and vendor-supported services contribute to regulatory readiness. Considered together rather than in isolation, the six themes indicate that participants do not experience vendor intelligence as a single undifferentiated input whose value can be assessed with a yes-or-no judgment. Instead, effectiveness, influence, and limitation function as three separable dimensions of the same underlying relationship between the organization and its vendors, and each research question surfaces a different one of those dimensions.

### *Research Question 1*

RQ1 asked how cybersecurity and compliance professionals within the G-SIB perceive the effectiveness of third-party threat intelligence in supporting regulatory readiness. As presented above, the findings show that, in participants' own accounts, effectiveness is conditional rather than fixed. Theme 1 (Contextual Relevance and Fit) and Theme 4 (Perceived Value) together indicate that participants judge a vendor's intelligence as effective largely to the degree that it is specific to the firm's actual business lines, geography, and risk exposure rather than generic industry-level reporting. At the same time, participants repeatedly separated evidentiary sufficiency, meaning documentation a regulator will accept, from a substantive

improvement in the organization's underlying security posture, and these two forms of value did not always move together; P09's and P12's accounts of evidentiary value above are the clearest illustration of this split. Theme 5 (Data-Quality Variability) further complicates the effectiveness judgment: participants described needing to actively verify, contextualize, and, at times, correct vendor output before treating it as usable evidence, which means perceived effectiveness is partly a function of the receiving organization's own verification capacity rather than the vendor's output quality alone. Taken together, RQ1 findings support a contingent, multidimensional model of effectiveness in which vendor intelligence is judged useful to the extent that it is organization-specific, independently corroborated, and clearly tied to a defined regulatory or operational outcome, a conclusion consistent with information governance research indicating that the value of external information artifacts is constructed through use rather than inherent in the artifact itself (Tallon et al., 2013).

### *Research Question 2*

RQ2 asked how decision-makers describe the role of third-party vendors in influencing regulatory readiness planning, assessment consistency, and investment decisions. As Theme 2 documents above, vendor influence on planning is exercised less through open competitive evaluation of intelligence quality and more through structural channels: regulator-approved vendor and accreditation lists, such as CBEST- and TIBER-recognized providers, informal reputational referral networks, and contractual statement-of-work compliance. This pattern indicates that, for a substantial share of participants, the vendor market that matters most operationally is defined by regulatory recognition rather than by independent efficacy testing, which reframes RQ2's question of vendor influence as a question of who controls the eligible vendor pool rather than who selects the best-performing one. Assessment consistency, in turn, is

constrained less by vendor quality than by the structural and governance fragmentation documented in Theme 3: P13's account of a first-line and second-line knowledge gap, and P10's observation that the organization governs the team that consumes third-party intelligence without governing the intelligence itself, both show that the same vendor-supplied intelligence can be integrated thoroughly in one part of the organization and remain largely invisible in another. On investment decisions specifically, participants offered comparatively little unprompted discussion of formal cost-benefit reasoning, which is itself a finding. The most plausible reading, though it is an inference rather than direct evidence, is that investment justification for vendor-supported regulatory readiness services may be handled upstream of the practitioners interviewed for this study, in procurement, sourcing, or senior leadership functions, rather than treated as a live consideration by the GRC and cybersecurity professionals who consume vendor output day to day; because no participants from procurement, sourcing, or senior leadership were interviewed directly, this remains an inference drawn from an absence in the data rather than a confirmed finding.

### *Research Question 3*

RQ3 asked what challenges or limitations participants identify when using third-party intelligence for regulatory examination preparation. Consistent with the findings presented above, generic or insufficiently contextualized intelligence (Theme 1) was the most frequently cited substantive limitation, particularly among participants operating at enterprise scale or across multiple jurisdictions. Structural and governance fragmentation (Theme 3) was the second recurring limitation, with onboarding lead times, information silos, and disconnected data systems repeatedly cited as constraints that persist independent of any single vendor's performance; P15's description of exercise reporting and control-gap findings scattered across

disconnected spreadsheets and platforms, and P09's account of nine-to-twelve-month onboarding timelines colliding with sixty-day regulatory windows, both illustrate this constraint concretely. Data-quality variability (Theme 5), particularly false positives and inconsistent vendor staffing and maturity, imposed a third, recurring validation burden that several participants described as lost analyst time and eroded trust. Theme 6 introduced a fourth, prospective limitation that the original research design had not anticipated on this specific dimension: the risk of unvalidated AI-generated content entering the regulatory-readiness pipeline without adequate human oversight, a concern participants raised proactively rather than in direct response to the interview's AI-capability question. Taken as a set, RQ3 findings indicate that the challenges participants associate with third-party CTI are not primarily a story about vendor performance. A meaningful share of the limitation originates inside the receiving organization itself, in its capacity to integrate, reconcile, and independently verify what vendors, and increasingly AI tools, provide; in this respect, RQ3's findings relocate part of the problem from the vendor to the organization that consumes the vendor's output.

### *The Research Framework*

Chapter 2 introduced a four-component conceptual framework depicting how third-party CTI and vendor-supported regulatory-readiness tools, treated as external inputs, are engaged by organizational actors, operationalized through governance and decision processes, and ultimately reflected, or not reflected, in regulatory readiness outcomes. The findings from this study largely confirm the framework's core proposition that vendor intelligence does not translate directly into readiness outcomes but rather depends on the organization's intervening judgment and governance capacity. Examining each component in turn clarifies both where the framework holds and where the empirical findings add nuance that the framework did not originally specify.

### *External Inputs*

The framework treats third-party CTI and vendor-supported tools as inputs rather than outcomes, cautioning that external intelligence does not inherently generate governance value independent of how it is engaged. Theme 1 substantiates this directly: participants consistently distinguished between the raw intelligence a vendor supplied and the tailored, verified version of that intelligence their organization actually used, and P07's and P08's accounts above both indicate that identical vendor output could be treated as more or less valuable depending entirely on how well it had been contextualized to the firm's specific business lines and jurisdictions. This finding is consistent with the framework's positioning of vendor services as inputs whose value is realized, or not realized, downstream.

### *Organizational Actors*

The framework's second component identifies cybersecurity, GRC, and risk management professionals as the interpretive layer that translates vendor intelligence into regulatory-relevant evidence. This role was visible throughout the data presented above: P08 described actively shaping and discarding vendor-proposed threat scenarios that did not fit the organization's actual business model, P12 described correcting inaccuracies in a vendor-generated risk-rating report before it reached a prospective business contact, and P03 described actively reconciling vendor questionnaire attestations against independent tool findings rather than accepting either at face value. The consistency of this interpretive activity across participants in different functional roles, including red-team, vulnerability-management, and GRC positions, supports the framework's premise that regulatory-readiness value is socially constructed by these actors rather than delivered ready-made by the vendor.

### *Governance and Decision Processes*

The framework identifies this component as a likely source of uncertainty, where misalignment between vendor output and internal governance can lead to inconsistent assessments and diminished confidence. Theme 3 is, in effect, an empirical elaboration of this exact mechanism. P13's description of a first-line and second-line information silo, in which second-line oversight has limited visibility into intelligence that the first-line CISO organization holds tightly, and P10's related observation that the organization governs the team consuming third-party intelligence without governing the intelligence itself, together describe precisely the kind of translation-layer breakdown the framework anticipated in general terms. Where the framework described this risk abstractly, the findings supply a specific organizational mechanism, fragmentation across systems, governance layers, and reporting lines, through which the risk materializes. In this respect, the findings do more than confirm the framework's prediction of uncertainty; they refine it, replacing a general expectation of misalignment with a specific, named mechanism, structural and governance fragmentation, that the original framework did not itself specify.

### *Regulatory Readiness Outcomes*

The framework's final component, comprising perceived examination preparedness, assessment consistency, and cost efficiency, was reflected unevenly in the findings. Examination preparedness and assessment consistency were well represented, particularly through Theme 4's emphasis on evidentiary sufficiency and Theme 2's emphasis on regulator-driven vendor selection criteria. Cost efficiency, by contrast, was largely absent from participants' unprompted accounts. This absence is more plausibly a function of who was sampled than evidence that cost efficiency is not a meaningful readiness outcome: this study's purposive sample was drawn from

practitioner-level cybersecurity, risk, and compliance roles, and cost-efficiency judgments more likely sit with procurement, sourcing, or senior leadership functions outside that sampling frame, consistent with the RQ2 observation above that investment justification appears to sit outside the practitioner-level vantage point captured by this study's sample. This represents a gap between what the framework specifies and what this sample was positioned to speak to, rather than a gap in the framework itself, and it is addressed further in the discussion of anticipated themes below.

### *Anticipated Themes*

Prior to data collection, Chapter 3 established a preliminary coding structure derived from the conceptual framework and literature review, comprising five a priori codes: Vendor Intelligence Value, Governance Integration, Regulatory Readiness Outcomes, Vendor Dependency Risk, and Cost and Investment Justification. Comparing this anticipated structure against the six themes that emerged through Braun and Clarke's (2022) inductive, six-phase thematic analysis process surfaces several points of convergence, divergence, and omission that are themselves informative about the phenomenon under study.

Two of the anticipated codes converged closely with emergent themes, though in each case the data sharpened or reframed the original construct. Vendor Intelligence Value anticipated something close to Theme 4 (Perceived Value: External Validation, Specialized Access, and Evidentiary Support), but the emergent theme proved considerably more specific than the a priori code implied: participants rarely described value in terms of raw intelligence quality and instead located it in unbiased outside perspective, access to specialized talent and scale, and, most consistently, evidentiary documentation sufficient to satisfy a named regulatory requirement. Governance Integration anticipated something resembling Theme 3 (Structural and Governance Fragmentation), but here the direction of the finding diverged meaningfully from what the a

priori code implied. The coding structure anticipated a theme on how intelligence outputs are incorporated into governance processes; participants instead described how that incorporation routinely fails due to system fragmentation, onboarding delays, and disconnected first- and second-line functions. What was anticipated as a theme of integration emerged, in practice, as a theme of fragmentation.

The a priori structure also anticipated two constructs that did not emerge as standalone themes in the final analysis. Regulatory Readiness Outcomes was anticipated as its own category, but, as discussed above, was distributed across multiple emergent themes, principally Themes 2 and 4, rather than standing on its own, an artifact of the fact that outcomes were something participants discussed in relation to specific vendor practices rather than as an independent topic. More notably, Cost and Investment Justification was substantially underrepresented in the data. Despite being anticipated as a distinct code grounded in the study's problem statement, participants offered little unprompted commentary on cost-benefit reasoning or formal investment justification, a gap consistent with the RQ2 finding that this dimension of vendor governance appears to sit above the practitioner vantage point represented in this study's purposive sample. Vendor Dependency Risk, the fifth a priori code, was partially reflected in Theme 5 (Data-Quality Variability) and Theme 2 (Vendor Selection and Evaluation Criteria) but reframed around vendor maturity variance and evaluation rigor rather than dependency in the narrower sense the code anticipated: concern about the organization's capacity to verify and select vendors well, rather than concern about over-reliance itself.

The clearest unanticipated theme was Theme 6 (Artificial Intelligence as an Emerging Complement, Not a Replacement). No a priori code addressed artificial intelligence at all, reflecting the state of the literature at the time the coding structure was developed. The interview

protocol did include a closing question about AI-driven internal capabilities, so the topic of AI was not absent from the data collection design; what was genuinely unanticipated was the specific content the theme ultimately centered on. As noted above, the concern that came to define Theme 6, namely the risk of unvalidated AI output entering a regulator-facing artifact without adequate human review, was raised proactively by participants rather than solicited by a direct question about AI risk. The theme is therefore unanticipated on two distinct levels: it was absent from the a priori coding scheme, and even the specific dimension that gave the theme its analytic weight emerged inductively rather than in response to a targeted prompt. Several participants described early efforts to deliberately bound experimentation with generative AI tools, paired with internally developed verification methodologies, such as P18's audited prompt-based control-mapping exercise and P10's managing-director-reviewed response-drafting tool, while explicitly cautioning against submitting AI output to a regulatory pipeline without that verification layer. Others, such as P08, described no internal AI evaluation of this kind and continued to rely on third-party providers specifically because of their perceived independence from internal technology and internal stakeholders. This range of responses, from active, governed experimentation to explicit reliance on third-party independence as a safeguard, suggests that AI is beginning to reshape how professionals think about vendor dependency itself, not simply adding a new vendor category but altering the terms on which the value of any external intelligence source, human or algorithmic, is evaluated. Framed against this study's central concern, AI's relevance here is not a freestanding technology trend but a new variant of the same third-party evidentiary question this study set out to examine: whether externally, or now algorithmically, produced intelligence can be trusted as regulator-facing evidence without independent, organization-level verification.

Because Theme 6 emerged inductively rather than from the a priori framework, interpreting it draws on recent industry literature that was not part of the original Chapter 2 review; this literature, cited for the first time in this discussion, is introduced specifically to help situate an emergent finding, not to suggest it informed the study's original design. This shift toward AI-augmented and AI-supplied intelligence is not occurring in a vacuum; it is unfolding alongside a rapidly changing external threat landscape in which the tools used to discover software vulnerabilities are increasingly capable of exploiting them. Recent industry analysis has documented a sharp compression in the gap between vulnerability disclosure and exploitation, with median time-to-exploit falling from roughly a year in 2021 to near zero in 2026, even as organizational patch and remediation timelines have not kept pace (Cembalest, 2026). The same analysis finds that the most advanced AI-assisted defensive tooling is often confined to vendor contracts, meaning the strongest detection and remediation capabilities may reside disproportionately with vendors serving larger, better-resourced clients (Cembalest, 2026). This dynamic offers a plausible external explanation for why participants in this study, several of whom described experimenting cautiously with AI rather than trusting it outright, treated AI-augmented vendor capability as an emerging rather than settled source of readiness value: the technology is moving quickly enough that neither the vendors nor the receiving organizations described in this study appear to have fully worked out governance norms for it yet.

### *The Problem*

The specific problem this study addressed was that the G-SIB may lack evidence that costly third-party threat intelligence and vendor-supported regulatory readiness services meaningfully improve examination preparedness, producing uncertainty in cybersecurity governance and complicating investment and risk management decisions. The findings speak

directly to this problem, though not in a way that resolves it cleanly in either direction. Participants did not describe vendor intelligence as ineffective; several described it as necessary, in some cases because regulators explicitly require third-party involvement to preserve independence and avoid the appearance of bias, as P17's account of regulator-mandated third-party testing illustrates. Necessity and demonstrated readiness improvement are not the same claim, however, and the findings show participants themselves drawing this distinction. The recurring separation between evidentiary sufficiency and substantive security improvement, most visible in Theme 4 and articulated most sharply by P09 and P12 above, deserves particular emphasis rather than passing mention: it is essentially a practitioner-level restatement of the evidentiary gap that motivated this study, and arguably the clearest single expression of that gap anywhere in the findings. Professionals on the ground can point to a folder of vendor documentation that satisfies an examiner. However, they cannot point to comparable confidence that the organization's underlying readiness has measurably improved as a result. This distinction, between documentation sufficient to pass an exam and evidence sufficient to establish genuine security improvement, is the crux of the problem this study set out to investigate.

The findings also complicate the problem statement's implicit framing of vendor value as a single evaluative question. Theme 3's fragmentation finding suggests that even where a vendor's intelligence is substantively strong, the organization's own governance architecture may prevent that value from accumulating into an institutional asset; P15's account of exercise findings scattered across disconnected spreadsheets and platforms shows how value can be realized once, within a single exercise, and then lost because no system captures and carries it forward to the next one. This reframes the applied business problem in a way the original

problem statement anticipated only implicitly: the evidentiary gap this study set out to examine is not solely a question of whether vendors deliver value, but also a question of whether the organization's internal governance processes are structured to retain and compound whatever value vendors do deliver. Addressing the problem may require investment in internal governance integration as much as investment in vendor selection itself, a practical implication with direct relevance to the G-SIB's cybersecurity investment and vendor governance decisions.

### *The Literature*

The findings both extend and, in a few respects, push back against the literature reviewed in Chapter 2 on the evolution of cybersecurity regulatory expectations, cyber threat intelligence and decision-making under regulatory scrutiny, and third-party risk management and vendor dependency.

Consistent with prior study, the findings reaffirm that information value is not inherent in an intelligence artifact but is constructed through organizational interpretation (Tallon et al., 2013) and that intelligence effectiveness is deeply entangled with organizational and regulatory context rather than being a fixed property of the intelligence itself (Ainslie et al., 2023). Participants' insistence on distinguishing generic from firm-specific intelligence and their active work to correct and contextualize vendor output before use closely mirror this literature's central claim that CTI's value depends on its integration into organizational sense-making rather than on its technical sophistication alone. The findings also align with regulatory guidance emphasizing operational resilience and structured cyber risk governance as the intended purpose of external intelligence investment (Basel Committee on Banking Supervision, 2021; National Institute of Standards and Technology, 2024). Theme 2 documents this regulator-driven pattern operating almost exactly as this literature would predict, with participants describing regulator-approved

provider lists, required accreditations, and jurisdiction-specific reporting formats as binding constraints on vendor selection well before any question of intelligence quality arises, a pattern formalized directly in the intelligence-led testing regimes participants referenced: the Bank of England's CBEST program (Bank of England, 2024), the European Central Bank's TIBER-EU framework (European Central Bank, 2018), and the Monetary Authority of Singapore's Technology Risk Management Guidelines (Monetary Authority of Singapore, 2021).

Where the findings diverge from the literature is chiefly in emphasis and specificity rather than outright contradiction. The literature on vendor dependency largely frames the central risk as overreliance on a single provider or category of providers. The findings from this study suggest a related but distinct risk that the existing literature addresses less directly: fragmentation across multiple vendor relationships and internal systems, rather than dependency on any one vendor, emerged in Theme 3 as participants' more salient governance concern. This is a meaningful refinement rather than a contradiction of the literature. However, it does suggest that vendor governance frameworks calibrated primarily around single-vendor dependency risk may be incompletely specified for an organization of this scale and vendor-relationship complexity.

A second point of productive tension concerns the concentration risk associated with vendor-supplied algorithmic and AI-driven tools, specifically, a topic largely absent from the Chapter 2 literature review, given how recently these tools have matured. Recent large-scale empirical research on algorithmic hiring tools offers a useful, if adjacent, illustration of the mechanism at stake: when many organizations rely on outputs from the same small number of third-party algorithmic vendors, correlated errors and blind spots can propagate across the entire population of client organizations in ways that would not be visible from any single vendor relationship examined in isolation, a pattern the researchers term an algorithmic monoculture

(Bommasani et al., 2026). Although that research examined employment screening rather than cyber threat intelligence, the underlying structural concern offers a useful parallel, rather than a direct transfer of findings, to this study's context: if G-SIB peer institutions increasingly draw on a small number of concentrated CTI or AI-augmented vendor platforms, an analogous concentration dynamic could plausibly emerge, with false-positive and vendor-maturity patterns similar to those documented in Theme 5 recurring across the sector rather than being independently distributed, a systemic dimension of vendor dependency that the existing third-party risk literature, and the original conceptual framework, do not explicitly model. This is precisely the kind of unanticipated, cross-cutting risk that Theme 6 gestures toward, but that participants, focused on their own organization's practices, were not positioned to observe directly. It represents a promising direction for future research, as recommended in this discussion.

Finally, the findings extend the literature's treatment of the relationship between AI capability and vendor value in ways that are only beginning to be documented in current industry analysis. Contemporary reporting on frontier AI models capable of both discovering and remediating software vulnerabilities describes a widening gap between attacker speed and organizational patch response, alongside a related concern that the strongest AI-assisted defensive capability is concentrated among vendors serving well-resourced clients (Cembalest, 2026). This pattern helps explain, rather than merely echo, the cautious posture toward AI that characterized Theme 6: participants' emphasis on internally developed verification methodology before trusting AI-generated output, illustrated above by P18's audited prompt and P07's warning against unreviewed AI submissions, is a reasonable governance response to an environment in which the underlying technology is advancing faster than the norms for evaluating it. While

Chapter 2's literature review necessarily treated CTI vendor relationships as relatively static, this study's findings, read alongside current developments, suggest that the literature would benefit from treating vendor-supplied intelligence and internally developed AI capabilities as increasingly interdependent and rapidly evolving rather than as separate, stable categories.

### *Synthesis*

Read together, the research questions, the conceptual framework, the anticipated coding structure, the problem statement, and the surrounding literature all point toward the same underlying interpretation: within this G-SIB, the regulatory-readiness value of third-party cyber threat intelligence is real but conditional, realized only to the extent that organizational actors and governance processes successfully translate external input into usable, retained institutional knowledge. The findings confirm the conceptual framework's core structure while sharpening several of its components, reframing governance integration as a site of fragmentation rather than assumed integration, and surfacing AI-augmented practice as an emergent factor that the original framework and coding structure did not anticipate. These refinements do not undermine the study's design; they are, in a qualitative single-case study, exactly the kind of context-specific elaboration the design was intended to surface (Yin, 2018; Hancock et al., 2021). The implications of these findings for practice, theory, and future research are addressed in the sections that follow.

## Implications and Recommendations for Future Research

### *Implications Introduction*

The discussion now turns from the study's findings to their broader significance, examining the practical, theoretical, and future-research implications of those findings, and considering how the study's own limitations may have shaped the specific pattern of results reported here. The inquiry took the form of a qualitative single-case study, exploring how cybersecurity, risk, and compliance professionals within a globally systemically important bank (G-SIB) evaluate the regulatory-readiness value of third-party cyber threat intelligence (CTI) and vendor-supported services. Findings were drawn from 18 interviews and 39 survey respondents, analyzed through Braun and Clarke's (2022) six-phase thematic analysis, and organized around six themes: contextual relevance and fit; vendor selection and evaluation criteria; structural and governance fragmentation; perceived value, encompassing external validation, specialized access, and evidentiary support; data-quality variability; and artificial intelligence's emerging role as a complement to, rather than a replacement for, professional judgment. These six themes anchor the implications discussed in the sections that follow.

### *Implications for Practice*

The findings point to several concrete adjustments that practitioners can make to the evaluation, governance, and reporting of third-party CTI and vendor-supported services. First, evidentiary sufficiency and substantive security improvement should be treated as two separate metrics rather than folded into a single composite score. Themes 1 and 4 suggest that a vendor's contribution to examination readiness and its contribution to measurable risk-posture change do not move in lockstep, and organizations that collapse the two into a single score risk obscuring which value a given engagement delivers. Board- and executive-level vendor reporting should be

built around this distinction, presenting examination-readiness value and risk-posture change as dual, independently tracked metrics.

Second, internal governance integration deserves investment at least as much as vendor selection itself. Theme 3's findings on structural and governance fragmentation point to consolidated intelligence repositories, clearly defined handoff protocols between first- and second-line functions, and cross-jurisdictional reporting standards as practical remedies. A particular priority is closing the gap between vendor onboarding timelines, which commonly run 9 to 12 months, and regulatory response windows that can be as short as 60 days; without governance integration to bridge that gap, even a well-selected vendor may not be operationally usable when it is needed most.

Third, organizations should supplement regulator-driven vendor accreditation frameworks, such as CBEST and TIBER, with a documented internal evaluation methodology. Theme 2 suggests that accreditation status alone is an incomplete proxy for vendor value; practitioners should also score vendors on contextual relevance to the organization's specific risk profile, a demonstrated track record of data quality, and the operational burden of integrating the vendor's outputs into existing workflows (Bank of England, 2024; European Central Bank, 2018).

Finally, organizations should formalize AI governance protocols before AI-assisted content is allowed to enter the regulatory readiness pipeline. Theme 6 indicates that artificial intelligence is being used as a complement to, not a substitute for, professional judgment, and that relationship needs explicit governance: verification protocols, human-review checkpoints, and clearly assigned accountability for any AI-generated content that informs regulatory-facing work.

### *Implications for Theory*

The findings refine, rather than displace, the four-component conceptual framework introduced in Chapter 2. Within that framework, the governance and decision-processes component is better characterized as structural and governance fragmentation rather than as a general misalignment risk; the data collected here point to a more specific failure mode than the framework originally anticipated. The outcomes component likewise benefits from refinement: evidentiary sufficiency and substantive security improvement emerge as distinct constructs that are only partially correlated, not two labels for the same underlying outcome. The framework should also be revised to treat vendor-supplied intelligence and AI-augmented capability as interdependent categories rather than as separate, stable ones, a revision motivated directly by Theme 6.

Beyond the conceptual framework, the study extends information governance theory by reinforcing that the value of an external information artifact is constructed through organizational use rather than fixed within the artifact itself (Tallon et al., 2013). A given piece of vendor intelligence is not inherently valuable or not; its value is realized, or left unrealized, by how the receiving organization is structured to use it. The study also extends third-party and vendor-dependency theory beyond the conventional concern with single-vendor overreliance. The findings introduce fragmentation and cross-platform concentration risk as a distinct hazard, one that parallels research on algorithmic monoculture in AI hiring contexts, where dependence on a small number of shared underlying models or platforms concentrates risk across otherwise independent organizations (Bommasani et al., 2026).

### *Implications for Future Research*

Several avenues for future research follow directly from this study's scope and its limitations. Future work could purposively sample procurement, sourcing, and senior-leadership roles, populations excluded from this study's practitioner-level sampling frame, to examine how CTI and vendor investment decisions are justified at the point where budget and strategy are set. A multi-case or comparative study, conducted across multiple G-SIBs or against regional banks and non-banking financial institutions operating under related regulatory regimes such as the Monetary Authority of Singapore's Technology Risk Management Guidelines (2021), would test whether the six themes identified here generalize beyond this single case (Yin, 2018; Hancock et al., 2021).

Future research could also empirically test vendor and AI platform concentration risk across G-SIB peer institutions, building directly on the algorithmic-monoculture parallel raised above (Bommasani et al., 2026). Finally, a longitudinal study tracking whether AI-governance maturity keeps pace with rapidly evolving AI-assisted vendor and defensive tooling would address the point-in-time limitation of Theme 6 and speak to a practice area that is likely to keep changing quickly (Cembalest, 2026).

### *Limitations of the Study and Their Influence on the Findings*

Several limitations shaped the specific pattern of findings reported here, and each is worth tracing explicitly rather than treating as a generic caveat. The study's purposive, practitioner-level sampling frame excluded procurement, sourcing, and senior-leadership roles. This exclusion plausibly explains the near-absence of cost-and-investment-justification data in the findings, despite the topic's inclusion in the a priori coding structure; the participants interviewed were not the people who make or justify those decisions.

A possible self-selection bias in voluntary participation is a second limitation (Robinson, 2014). Fifteen of the eighteen participants, or 83.3%, had ten or more years of experience, and this skew toward tenured practitioners may have amplified both Theme 3's structural-fragmentation critique and Theme 5's data-quality skepticism, views that more experienced practitioners may hold more strongly or articulate more readily than newer staff.

Confidentiality constraints also limited documentary triangulation. Figures such as onboarding timelines and the number of disconnected systems rely on participants' self-reports rather than independently verified records. The thematic patterns themselves remain well supported across the data, but the specific figures cited in this study should be read as informed perception rather than audited fact.

Finally, the single-case, single-institution design means the findings are analytically, rather than statistically, generalizable (Yin, 2018; Hancock et al., 2021). This bounded design leaves an open opportunity for a broader quantitative study to test whether these patterns hold beyond this single case, and it means Theme 6 should be read as a point-in-time snapshot of a fast-moving practice area rather than as a durable finding.

### *Implications Summary*

The regulatory-readiness value of third-party CTI is real, but it is conditional: it depends on an organization's governance capacity at least as much as on vendor performance. Accordingly, the conclusions offered here should be understood as an analytically rich, contextually bounded account of one institution's experience, not as a statistically generalizable claim about G-SIB practice.

### *Recommendations Introduction*

The recommendations that follow propose specific, evidence-based directions for future research that extend directly from the study's six themes and its bounded, single-case design, explaining why each recommended direction follows from what the study found. The inquiry took the form of a qualitative single-case study, exploring how cybersecurity, risk, and compliance professionals within a globally systemically important bank (G-SIB) evaluate the regulatory-readiness value of third-party cyber threat intelligence (CTI) and vendor-supported services. Findings were drawn from 18 interviews and 39 survey respondents, analyzed through Braun and Clarke's (2022) six-phase thematic analysis, and organized around six themes: contextual relevance and fit; vendor selection and evaluation criteria; structural and governance fragmentation; perceived value, encompassing external validation, specialized access, and evidentiary support; data-quality variability; and artificial intelligence's emerging role as a complement to, rather than a replacement for, professional judgment. These six themes anchor the implications discussed in the sections that follow.

### *Recommendation 1: Cross-Institutional Vendor and AI-Platform Concentration Risk*

Replicate this study's screening-survey-plus-interview design across multiple G-SIB peer institutions to test whether reliance on a small, overlapping set of CTI and AI-augmented vendor platforms produces correlated false-positive and data-quality patterns across the sector, paralleling documented algorithmic-monoculture effects in AI hiring tools (Bommasani et al., 2026). In the study, Theme 5 documented vendor-attributable data-quality variability and false positives as a persistent, operationally costly limitation for 12 of 18 participants (66.7%), and Theme 6 showed active reliance on AI-augmented vendor and internal tools without any visibility into whether other institutions draw on the same platforms; a single-case design can

describe this pattern within one G-SIB but cannot determine whether it is unique to this institution or systemic across the sector.

***Recommendation 2: Procurement, Sourcing, and Senior-Leadership Perspectives on Investment Justification***

Purposively sample procurement, sourcing, and senior- or executive-leadership roles directly, using Ahmad and Wilkins's (2025) purposive-sampling framework, to examine how CTI and vendor-support investment decisions are financially and strategically justified. This study's practitioner-level purposive sampling frame excluded procurement, sourcing, and senior leadership by design, and cost-and-investment-justification data were nearly absent from the interviews despite being included in the a priori coding structure; Theme 2's finding that vendor evaluation is driven chiefly by regulator-mandated accreditation, reputational vetting, and statement-of-work compliance, rather than an independent assessment of value, suggests that the financial reasoning behind these decisions sits above the vantage point this sample could reach.

***Recommendation 3: Multi-Case Comparison Across G-SIBs and Non-Bank Financial Institutions***

Replicate the six-phase thematic analysis (Braun & Clarke, 2022) across two or three additional G-SIBs, or contrast findings against regional banks or non-bank financial institutions operating under related regimes such as Singapore's Technology Risk Management Guidelines (Monetary Authority of Singapore, 2021), to test which of the six themes generalize beyond this institution. A single-case, single-institution design supports analytical rather than statistical generalization (Yin, 2018; Hancock et al., 2021); Theme 3's structural and governance fragmentation (information silos, disconnected systems, onboarding delays) and Theme 1's contextual-fit continuum were described in terms specific to this institution's structure. It is not

yet known whether these dynamics are sector-wide or artifacts of this organization's particular governance architecture.

A quantitative component would strengthen this recommendation by testing the drivers of investment justification rather than merely describing them. A structured survey administered to not only GRC professionals, but also to procurement, sourcing, and senior-leadership respondents, analyzed using standard quantitative methods, would allow the relative weight of factors such as regulatory mandate, cost, reputational risk, and demonstrated security value to be measured and compared across a larger, role-diverse sample, testing whether Theme 2's compliance-driven pattern holds more broadly rather than remaining a single-case qualitative observation.

***Recommendation 4: Longitudinal Tracking of AI-Governance Maturity***

A multi-wave longitudinal study (e.g., annual interviews or document review conducted over two to three years) tracking whether verification protocols, human-review checkpoints, and accountability structures for AI-generated regulatory content keep pace with the evolution of AI-assisted vendor and defensive tooling (Cembalest, 2026). Theme 6 is explicitly a point-in-time snapshot of a fast-moving practice area; participants' own caution, such as auditing AI-generated output before submission and warning against unreviewed AI content, reflects a governance response to a technology evolving faster than the norms for evaluating it, a dynamic that a single interview wave cannot capture.

### *Recommendation 5: Instrumentation to Separate Evidentiary Sufficiency from Substantive Security Improvement*

Develop and validate a measurement instrument, such as a dual-scale survey or structured audit rubric, that operationalizes evidentiary sufficiency and substantive security-posture improvement as distinct, measurable constructs, piloted within this G-SIB and then tested across additional institutions. This bifurcation is the study's central finding (Theme 4), articulated directly by participants as a distinction between documentation value and posture improvement; the qualitative design surfaced this distinction conceptually but was not intended to measure it, making instrument development the natural next empirical step rather than further replication alone.

### *Recommendations Summary*

Each recommendation follows directly from a specific theme or a bounded limitation of this study rather than from a generic call for more research. Pursuing these directions would test the generalizability of the six themes across institutions while extending the evidentiary-versus-substantive distinction from a qualitative finding into a measurable construct.

## Summary and Study Conclusion

This qualitative single-case study set out to examine how cybersecurity, risk, and compliance professionals within a large, U.S.-based G-SIB evaluate the regulatory-readiness value of third-party cyber threat intelligence and vendor-supported services, addressing a gap in the empirical literature on how organizational decision-makers determine whether such investments meaningfully contribute to regulatory readiness outcomes. Guided by three research questions addressing perceived effectiveness, vendor influence on planning and investment, and the challenges participants encounter in practice, the study analyzed 18 semi-structured interviews,

triangulating them with screening survey data from 39 respondents, using Braun and Clarke's (2022) six-phase thematic analysis procedure.

Six themes emerged from this analysis: Contextual Relevance and Fit; Vendor Selection and Evaluation Criteria; Structural and Governance Fragmentation; Perceived Value—External Validation, Specialized Access, and Evidentiary Support; Data-Quality Variability; and Artificial Intelligence as an Emerging Complement, Not a Replacement. Read together, these themes indicate that participants do not experience third-party CTI as a single input whose value can be assessed as simply effective or ineffective. Rather, effectiveness is conditional on contextual fit and independent verification; vendor influence is exercised largely through structural and regulatory channels rather than through open competitive evaluation; and the challenges participants identify originate as much within the receiving organization's own governance structure as in vendor performance itself. Central to these findings is the distinction, articulated directly by several participants, between evidentiary sufficiency and substantive security improvement: professionals can point to documentation that satisfies a regulatory examiner but cannot point to comparable evidence that the organization's underlying security posture has measurably improved. This distinction is, in effect, a practitioner-level restatement of the evidentiary gap that motivated the study, and it represents the clearest single answer this study offers to the applied business problem introduced in Chapter 1.

The findings both confirm and refine the conceptual framework introduced in Chapter 2, most notably by replacing a general expectation of governance misalignment with the specific, empirically grounded mechanism of structural and governance fragmentation, and by surfacing AI-augmented practice as an emergent factor that the original framework did not anticipate. Consistent with the interpretive aims of a qualitative single-case design, these conclusions are

offered as analytically, rather than statistically, generalizable: they describe how regulatory-readiness value is constructed within this particular institutional context, bounded by the assumptions, limitations, and delimitations described in Chapter 3, rather than as claims intended to generalize statistically to G-SIB institutions as a population (Yin, 2018; Hancock et al., 2021).

For an institution operating under continuous regulatory scrutiny while sustaining substantial investment in external cybersecurity intelligence, this study's contribution is to make visible a distinction that is easy to lose in day-to-day governance practice: documentation sufficient to satisfy an examiner and evidence sufficient to establish genuine security improvement are related, but separable achievements, and sustained regulatory readiness depends on organizations building the internal capacity to pursue both.

## References

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Ahmad, M., & Wilkins, S. (2025). Purposive sampling in qualitative research: A framework for the entire journey. *Quality & Quantity, 59*(2), 1461–1479. https://doi.org/10.1007/s11135-024-02022-5

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security, 132*, 103352. https://doi.org/10.1016/j.cose.2023.103352

Arena, M., Arnaboldi, M., & Palermo, T. (2019). The dynamics of (dis)integrated risk management: A comparative field study. *Accounting, Organizations and Society, 74*, 68–81. https://doi.org/10.1016/j.aos.2018.09.001

Bank of England. (2024). *CBEST threat intelligence-led assessments: Implementation guide for CBEST participants*. https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide

Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

Bernardo, B. M. V., Viana, B. N., & de Carvalho, M. M. (2024). Data governance & quality management—Innovation and future agenda: A systematic review. *Journal of Industrial Information Integration, 37*, 100519.

Bommasani, R., Bana, S. H., Creel, K. A., Jurafsky, D., & Liang, P. (2026, May 26). AI hiring tools can yield racial bias and systemic rejection. *Stanford Institute for Human-Centered Artificial Intelligence*. https://hai.stanford.edu/news/ai-hiring-tools-can-yield-racial-bias-and-systemic-rejection

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE Publications.

Caluwe, L., Wilkin, C. L., De Haes, S., & Huygh, T. (2024). Board roles are required for IT governance to become an integral part of corporate governance. *International Journal of Accounting Information Systems, 54*, 100694. https://doi.org/10.1016/j.accinf.2024.100694

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security, 105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Cembalest, M. (2026, July 22). Patchmageddon: The race to patch software vulnerabilities before zero-day cyber-exploitations proliferate. *J.P. Morgan Private Bank, Eye on the Market*. https://assets.jpmprivatebank.com/content/dam/jpm-pb-aem/global/en/documents/eotm/patchmageddon.pdf

Coglianese, C., & Lehr, D. (2019). Regulating by robot: Administrative decision making in the machine-learning era. *Georgetown Law Journal, 105*(5), 1147–1223.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE.

Creswell, J. W., & Guetterman, T. C. (2019). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (6th ed.). Pearson.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise governance of IT, business/IT alignment and value creation* (3rd ed.). Springer.

Didenko, A. N. (2020). Cybersecurity regulation in the financial sector: Prospects of legal harmonization in the EU and beyond. *Uniform Law Review, 25*(1), 125–167. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3533664

Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics, 145*(3), 802–826. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf

Enworo, O. C. (2023). Application of Guba and Lincoln's parallel criteria to assess trustworthiness of qualitative research on indigenous social protection systems. *Qualitative Research Journal, 23*(4), 372–384. https://doi.org/10.1108/QRJ-08-2022-0116

European Central Bank. (2018). *TIBER-EU framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

European Union Agency for Cybersecurity (ENISA). (2022). *ENISA threat landscape 2022*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Gartner. (2023). *Market guide for security threat intelligence products and services*. Gartner Research.

Hancock, D. R., Algozzine, B., & Lim, J. H. (2021). *Doing case study research: A practical guide for beginning researchers* (4th ed.). Teachers College Press.

Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews, 23*(1), 7–44. https://doi.org/10.1111/ijmr.12239

Lacity, M. C., & Willcocks, L. P. (2014). Business process outsourcing and dynamic innovation. *MIS Quarterly Executive, 13*(4), 205–219.

Li, T., No, W. G., & Wang, T. (2021). SEC cybersecurity disclosure guidance and firm disclosure behavior. *MIS Quarterly, 45*(2), 1–28.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review, 24*, 35-61. https://www.sciencedirect.com/science/article/abs/pii/S1574013716301137

McNulty, D. (2023). Data access technologies and the ‘new governance’ of financial regulation. *Journal of Financial Regulation, 9*(2), 225–255. https://academic.oup.com/jfr/article/9/2/225/7256156

Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative data analysis: A methods sourcebook* (4th ed.). SAGE.

Monetary Authority of Singapore. (2021, January 18). *Technology risk management guidelines*. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

National Institute of Standards and Technology. (2024). *Cybersecurity framework* (Version 2.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Oshri, I., Kotlarsky, J., & Willcocks, L. P. (2019). *The handbook of global outsourcing and offshoring* (4th ed.). Palgrave Macmillan.

PwC. (2025). *Global digital trust insights 2025: Accelerating digital trust*. PricewaterhouseCoopers. https://www.pwc.com/us/en/services/consulting/cybersecurity-data-tech-risk/library/global-digital-trust-insights.html

Ravitch, S. M., & Carl, N. M. (2021). *Qualitative research: Bridging the conceptual, theoretical, and methodological* (2nd ed.). SAGE.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*(1), 25–41. https://doi.org/10.1080/14780887.2013.801543

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data, 7*(1), 1–29. https://doi.org/10.1186/s40537-020-00318-5

Taddeo, M. (2019). Three challenges for ethical AI governance in cybersecurity. *Minds and Machines, 29*(3), 399–406. https://doi.org/10.1007/s11023-019-09504-8

Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems, 30*(3), 141–177. https://doi.org/10.2753/MIS0742-1222300306

Teece, D. J. (2019). A capability theory of the firm: An economics and (strategic) management perspective. *New Zealand Economic Papers, 53*(1), 1–43. https://doi.org/10.1080/00779954.2017.1371208

Thomas, G. (2021). *How to do your case study* (3rd ed.). SAGE.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, 72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Tracy, S. J. (2020). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (2nd ed.). Wiley-Blackwell.

Trainor, A. A., & Graue, E. (2022). *Reviewing qualitative research in the social sciences: A step-by-step guide*. Routledge.

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security, 87*, 101589. https://doi.org/10.1016/j.cose.2019.101589

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

Zibak, A., Sauerwein, C., & Simpson, A. C. (2022). Threat intelligence quality dimensions for research and practice. *Digital Threats: Research and Practice, 3*(4), Article 30. https://doi.org/10.1145/3484202

## Appendix A: List of Acronyms

| | |
|---|---|
| AI | Artificial Intelligence |
| BCBS | Basel Committee on Banking Supervision |
| CBEST | Critical National Infrastructure Banking Supervision and Evaluation Testing |
| CFPB | Consumer Financial Protection Bureau |
| CISO | Chief Information Security Office |
| CTI | Cyber Threat Intelligence |
| FFIEC | Federal Financial Institutions Examination Council |
| G-SIB | Globally Systemically Important Bank |
| GRC | Governance, Risk, and Compliance |
| IRB | Institutional Review Board |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| OCC | Office of the Comptroller of the Currency |
| ROI | Return On Investment |
| TI | Threat Intelligence |
| TIBER | Threat Intelligence-Based Ethical Red Teaming |

## Appendix B: Qualitative Data Analysis Procedures

Qualitative case study methodology supports the exploration of complex organizational phenomena within real-world contexts and allows researchers to examine decision-making processes, governance practices, and experiential perspectives in depth (Creswell & Creswell, 2023; Thomas, 2021; Yin, 2018). Data collected through semi-structured interviews will be analyzed using thematic analysis to identify patterns and recurring constructs across participant experiences (Braun & Clarke, 2022).

Interview transcripts will be analyzed using the six-phase thematic analysis approach proposed by Braun and Clarke (2022). The researcher will first become familiar with the data by repeatedly reading the interview transcripts. Initial codes will then be generated to capture meaningful segments related to regulatory readiness, third-party intelligence utilization, governance decision-making, and vendor evaluation processes. Codes will be grouped into candidate themes representing recurring concepts across participant responses. Themes will then be reviewed and refined to ensure internal consistency and alignment with the conceptual framework.

## Appendix C: Project Type & Organization Permission

To Byron Busby,

This letter serves to confirm my approval for you to conduct your doctoral research project, "Evaluating the Effectiveness of Third-Party Threat Intelligence in Supporting Cyber Regulatory Readiness," [redacted] You have my permission to invite eligible employees to participate in your study, provided that all research activities adhere to the ethical standards outlined in your request.

I understand that this research is solely for academic purposes, and that neither the project nor its results will be published. I also acknowledge that participation is entirely voluntary, and that individual or organizational identifiers will not be disclosed, with all collected data handled in accordance with institutional ethical standards.

I look forward to discussing the study in greater detail and can provide a signed statement of approval as required.

Sincerely,

Signature [redacted] _ Date: March 13, 2026

[redacted]

Director, Cybersecurity Operations [redacted]

## Appendix D: Research Design Alignment Matrix

| Research Component | Description | Connection to the Study |
|---|---|---|
| Business Problem | Large, federally regulated G-SIB institutions invest substantially in third-party CTI and vendor-supported regulatory readiness services without clear empirical evidence that these investments improve regulatory examination preparedness. | This problem reflects a material governance uncertainty in cybersecurity compliance investment decisions within highly regulated institutions. |
| Specific Problem | G-SIB institutions may lack defensible, outcome-based evidence demonstrating whether costly third-party CTI and vendor-supported readiness services improve preparedness for cybersecurity regulatory examinations. | This gap creates uncertainty in vendor governance, compliance budgeting, and internal capability development strategy. |
| Purpose Statement | To explore how cybersecurity, risk, and compliance professionals within a U.S.-based G-SIB evaluate the regulatory-readiness value of third-party CTI and vendor-supported services through a qualitative single-case study. | The study examines how decision-makers interpret, evaluate, and integrate vendor-supported intelligence into regulatory readiness processes. |
| RQ1 | How do cybersecurity and compliance professionals perceive the effectiveness of third-party CTI in supporting regulatory readiness? | Examines professional perceptions of governance value and examination utility of vendor-supported intelligence. |
| RQ2 | How do decision-makers describe vendor influence on regulatory readiness planning, assessment consistency, and investment decisions? | Explores governance mechanisms through which vendor intelligence is operationalized and justified. |

| | | |
|---|---|---|
| RQ3 | What challenges or limitations do participants identify when using third-party CTI for regulatory examination preparation? | Identifies barriers constraining vendor intelligence from translating into examination-ready governance outcomes. |
| Data Collection | Semi-structured interviews with cybersecurity governance, compliance, and risk management professionals within the participating G-SIB institution. | Interviews enable participants to describe governance experiences, evaluative judgments, and professional perspectives in depth. |
| Data Analysis | Thematic analysis of interview transcripts using the six-phase Braun and Clarke (2022) procedure, supported by NVivo software. | Thematic analysis will identify recurring patterns in how professionals evaluate third-party CTI within regulatory readiness processes. |

*Note.* Developed by the researcher.

## Appendix E: Semi-Structured Interview Protocol

### *Opening Script*

Thank you for participating in this research study. The purpose of this interview is to understand how cybersecurity and governance professionals evaluate the regulatory-readiness value of third-party cyber threat intelligence and vendor-supported services. Participation is voluntary, and responses will remain confidential. The interview will take approximately 30–45 minutes.

1. Can you describe your role in supporting cybersecurity regulatory readiness within your organization and how vendor-supported intelligence or advisory services fit into that process?

2. From your experience, how does third-party cyber threat intelligence influence regulatory readiness planning, control assessments, or examination preparation within your organization?

3. From your perspective, what value do these third-party services provide in preparing for cybersecurity regulatory examinations?

4. What factors do you or your organization consider when evaluating whether vendor-provided threat intelligence or readiness services are effective for regulatory preparedness?

5. What challenges or limitations have you observed when using third-party intelligence or vendor-supported services during regulatory readiness activities or examination preparation?

6. Based on your experience, what improvements could organizations make to better integrate external threat intelligence into cybersecurity governance and regulatory readiness processes?

7. Have you or your organization evaluated any internally developed or AI-driven alternatives to third-party intelligence services? If so, how do they compare?

### *Closing Question*

Is there anything else you believe is important for understanding how organizations evaluate the effectiveness of third-party cyber threat intelligence in supporting regulatory readiness?

## Appendix F: Preliminary Qualitative Coding Framework

| Code | Description | Example Evidence |
|---|---|---|
| Vendor Intelligence Value | Participant perceptions of the usefulness or relevance of third-party CTI. | Statements describing benefits of vendor intelligence for exam preparation. |
| Governance Integration | How intelligence outputs are incorporated into internal governance processes. | References to risk assessments, compliance documentation, or board reporting. |
| Regulatory Readiness Outcomes | Perceived impact of CTI on examination preparedness and assessment consistency. | Descriptions of improved documentation, audit readiness, or regulatory confidence. |
| Vendor Dependency Risk | Concerns about over-reliance on third-party providers. | Comments about reduced internal capability or unclear accountability. |
| Cost and Investment Justification | How organizations evaluate the financial value of CTI services. | Discussion of budgeting decisions or ROI uncertainty. |

*Note.* Developed by the researcher.