Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 4 No. 1 (2026)

Evaluating How Cybersecurity Threat Intelligence Enhances AI-Driven Risk Assessment in Internal Auditing

[1]Muhammad Rashid Mahmood
[2]Dr. Shahid Naseem
[3]Khan Imdad Ullah
[1]PhD Scholar, Lincoln University College, Malaysia
[2]Assistant Professor (IT), University of Education Township Lahore, Pakistan
[3]PhD Scholar, Lincoln University College, Malaysia
[1]rashidtalha1@gmail.com, [2]shahid.naseem@ue.edu.pk, [3]Khanimdadullah@yahoo.com

Abstract

The increasing adoption of artificial intelligence (AI) in internal auditing has transformed risk assessment practices, enabling continuous monitoring, predictive analytics, and data-driven audit planning. However, the effectiveness of AI-driven risk assessment in cyber-relevant domains remains uneven, often producing misleading signals or false confidence when applied without sufficient contextual understanding of the external threat environment. This study examines how cybersecurity threat intelligence (CTI) enhances the effectiveness of AI-driven risk assessment in internal auditing. Grounded in Information Processing Theory, the study develops a theory-driven conceptual framework explaining how CTI and AI function as complementary capabilities that jointly reduce environmental uncertainty. AI-driven analytics expand information processing capacity, while CTI enhances information richness by providing external context, interpretive meaning, and anticipatory insight into evolving cyber threats. The framework specifies direct effects of CTI on audit risk assessment effectiveness, mediating mechanisms of contextual enrichment and signal-to-noise improvement, moderating effects of AI integration maturity and governance, and dynamic feedback effects over time. The framework is analytically applied across varying levels of CTI maturity, demonstrating non-linear threshold effects in which meaningful improvements in audit risk assessment effectiveness emerge only when intelligence quality, integration, and governance reach sufficient maturity. The analysis further identifies key failure modes, including intelligence noise amplification, automation bias, and feedback-loop path dependence, and proposes concrete governance and control mechanisms to mitigate these risks. This study contributes to the literature by extending Information Processing Theory to internal audit risk assessment under cyber uncertainty, introducing cybersecurity threat intelligence as a foundational antecedent to AI-driven audit analytics, and providing a structured roadmap for responsible adoption. For practice, the findings underscore that the value of AI in internal auditing depends not only on algorithmic sophistication but on the quality, relevance, and governance of the intelligence that informs it.

Keywords: Cybersecurity threat intelligence; AI-driven risk assessment; Internal auditing; Audit analytics; Cyber risk governance; Information Processing Theory; Artificial intelligence governance; Continuous auditing

Article Details:

Received on 22 Dec, 2025
Accepted on 20 Jan, 2026
Published on 22 Jan, 2026

Corresponding Authors*

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 4 No. 1 (2026)

1. Introduction

1.1 Cyber Risk, Threat Intelligence, and the Expanding Role of Internal Audit

Organizations increasingly operate in digital environments characterized by extensive interconnectivity, rapid technological change, and persistent cyber threats. Contemporary cyber risks are rarely isolated technical incidents; rather, they reflect coordinated, evolving threat activity with direct implications for organizational governance, financial integrity, operational resilience, and reputation. As cyber incidents continue to escalate in frequency and sophistication, boards and audit committees increasingly expect internal audit functions to provide credible and forward-looking assurance over cyber-related risks [8], [14]. Meeting these expectations requires more than internal visibility into systems and controls. Cyber threats are shaped by external actors, attack campaigns, and vulnerabilities that often emerge beyond organizational boundaries. Consequently, **cybersecurity threat intelligence (CTI)**—the systematic analysis of information about threat actors, techniques, and campaigns—has become a critical input for understanding the external risk environment [1], [2]. Internal audit functions, however, have only begun to engage with CTI as part of their risk assessment processes.

1.2 Limitations of Traditional Internal Audit Risk Assessment

Traditional internal audit risk assessment approaches were developed for relatively stable environments in which risks evolve incrementally and historical data provide meaningful guidance for future exposure. Periodic risk assessments, management interviews, prior audit findings, and control self-assessments remain foundational practices, but their limitations are increasingly apparent in the context of cyber risk.

Cyber threats evolve rapidly, exploit previously unknown vulnerabilities, and are deliberately concealed by threat actors. As a result, retrospective indicators may fail to signal emerging risks until after control failures or incidents have occurred [1], [2]. Prior research indicates that internal audit functions often struggle to prioritize cyber risks consistently and to communicate their significance effectively to audit committees, particularly when risks originate outside the organization's immediate control environment [10], [14]. These limitations have prompted calls for more dynamic, data-driven approaches to audit risk assessment that can operate under conditions of high uncertainty.

1.3 Emergence and Limits of AI-Driven Risk Assessment

In response, internal audit functions have increasingly adopted **AI-driven risk assessment** techniques. Machine learning models, predictive analytics, anomaly detection, and continuous monitoring systems enable internal audit to analyze large volumes of transactional, operational, and security-related data in near real time [15]–[17]. These tools promise improved risk identification accuracy, reduced detection latency, and more frequent reassessment of risk priorities.

However, experience from both research and practice suggests that AI-driven risk assessment does not consistently deliver these benefits. Organizations deploying similar analytical tools often report divergent outcomes, including excessive false positives, blind spots related to novel threats, and overconfidence in automated risk scores [18], [21]. These limitations reflect a fundamental constraint: AI systems expand analytical capacity but remain dependent on the quality, relevance, and interpretability of their input data. In cyber contexts, where malicious behavior is adversarial and intentionally deceptive, internal data alone may be insufficient to provide meaningful signals. Without external threat context, AI-driven risk assessment may misclassify benign anomalies as significant risks or, more critically, normalize emerging threats as routine activity.

https://doi.org/10.5281/zenodo.18336904

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

1.4 The Role of Cybersecurity Threat Intelligence in AI-Supported Auditing

Cybersecurity threat intelligence addresses this limitation by enriching analytical processes with external context. CTI provides structured, analyzed information about threat actors, attack techniques, campaigns, and vulnerabilities, enabling organizations to interpret internal signals in light of the broader threat landscape [1], [2]. Empirical research in cybersecurity operations demonstrates that CTI improves detection accuracy, prioritization, and anticipatory risk management when it is relevant and well governed [8], [11].

Despite these benefits, CTI remains under-integrated into internal audit risk assessment. Audit analytics research has largely focused on internally generated data and algorithmic techniques, with limited attention to how external intelligence shapes audit judgment. As AI-driven risk assessment becomes central to audit planning and risk prioritization, this omission raises concerns about the reliability and governance relevance of AI-supported audit outputs.

1.5 Research Gap and Objectives

Existing research has examined cybersecurity threat intelligence primarily in the context of security operations and incident response, while audit analytics studies have focused on the technical capabilities of AI systems. There is limited theoretical integration explaining how CTI influences AI-driven risk assessment within internal audit functions, the mechanisms through which intelligence improves audit judgments, or the conditions under which CTI enhances rather than distorts risk assessment.

This study addresses these gaps by examining **how cybersecurity threat intelligence enhances AI-driven risk assessment in internal auditing**. The objective is not to evaluate specific algorithms but to explain the informational and organizational mechanisms through which CTI improves the accuracy, timeliness, and reliability of AI-based audit risk assessments.

1.6 Theoretical Perspective and Contributions

The study is grounded in **Information Processing Theory**, which posits that organizational effectiveness depends on the alignment between environmental uncertainty and information processing capacity [29], [30]. Cyber threat environments impose exceptionally high uncertainty due to rapid change, adversarial intent, and incomplete information. AI-driven analytics increase processing capacity, while CTI enhances information richness by providing context, meaning, and anticipatory insight. Together, these capabilities enable internal audit functions to process cyber risk information more effectively than either capability alone.

This article makes four primary contributions. First, it positions CTI as a foundational input to AI-driven internal audit risk assessment, extending audit analytics research beyond internally focused data sources. Second, it explicates the mechanisms through which CTI enhances AI-based risk judgments. Third, it identifies moderating and dynamic effects related to AI integration maturity and governance. Finally, it highlights failure modes and governance controls necessary to prevent intelligence-induced bias and over-reliance on automated outputs.

1.7 Research Questions

To guide the analysis, this study addresses the following research questions:

RQ1: How does cybersecurity threat intelligence influence the effectiveness of AI-driven risk assessment in internal auditing?

RQ2: Through what mechanisms does cybersecurity threat intelligence enhance the accuracy, timeliness, and reliability of AI-based audit risk assessments?

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

RQ3: How do AI integration maturity and governance practices moderate the relationship between cybersecurity threat intelligence and AI-driven risk assessment effectiveness?
RQ4: How does continuous feedback between cybersecurity threat intelligence and AI-driven risk assessment affect audit risk assessment performance over time?

1.8 Structure of the Article

The remainder of the article is structured as follows. Section 2 reviews prior research on cybersecurity threat intelligence, internal audit risk assessment, AI-driven analytics, and information processing perspectives. Section 3 presents the theoretical foundation. Section 4 develops the conceptual framework and hypotheses. Section 5 outlines the research design. Section 6 applies the framework across CTI maturity levels. Sections 7 and 8 discuss theoretical and practical implications, including governance and risk considerations. Sections 9 and 10 conclude with limitations, future research directions, and final insights.

2. Background and Related Work

2.1 Cybersecurity Threat Intelligence: Concepts, Levels, and Maturity

Cybersecurity threat intelligence (CTI) has become an essential capability for organizations seeking to understand and manage cyber risk in increasingly hostile and uncertain digital environments. CTI is generally defined as the systematic collection, analysis, and dissemination of actionable information regarding cyber threats, including threat actors, their motivations, capabilities, tactics, techniques, and procedures, as well as the vulnerabilities and assets they target [1], [2]. A defining feature of CTI is its emphasis on interpretation and relevance rather than raw data volume; intelligence is valuable only insofar as it reduces uncertainty and informs decision-making.

Prior literature distinguishes CTI across multiple levels of abstraction. **Strategic threat intelligence** focuses on long-term trends, geopolitical developments, and systemic risk implications relevant to senior executives and boards. **Tactical intelligence** emphasizes adversary behaviors and attack techniques, often structured using frameworks such as MITRE ATT&CK [3]. **Operational intelligence** supports near-term defensive actions by identifying active campaigns, while **technical intelligence** consists of granular indicators of compromise such as IP addresses, domains, or file hashes [2], [12]. These distinctions reflect differences in time horizon, audience, and decision relevance.

Recent research has shifted attention from the mere availability of threat intelligence to **CTI maturity**. Mature CTI capabilities are characterized by curated and validated sources, relevance to organizational context, integration with internal telemetry, and continuous refinement through feedback [8], [10], [11]. Empirical studies indicate that low-quality or poorly contextualized intelligence can overwhelm analysts and degrade analytical performance, whereas high-quality intelligence improves prioritization and reduces false signals [9], [10]. Despite this growing body of work, CTI research remains largely anchored in security operations and incident response. The role of threat intelligence in governance and assurance functions—particularly internal auditing—has received limited theoretical and empirical attention.

Research gap: Existing CTI literature does not explain how threat intelligence maturity influences AI-supported risk assessment within internal audit functions or how intelligence quality affects audit judgment and assurance outcomes (RQ1, RQ2).

2.2 Risk Assessment in Internal Auditing

Risk assessment is a foundational activity in internal auditing, shaping audit planning, resource allocation, and reporting priorities. Traditional internal audit risk assessment relies on management interviews, historical loss data, prior audit findings, and control self-

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

assessments [13], [14]. These approaches assume relatively stable risk conditions and the availability of observable indicators that can be extrapolated into future risk estimates.

Cyber risk challenges these assumptions in fundamental ways. Cyber threats evolve rapidly, often originate outside organizational boundaries, and may remain undetected for extended periods. As a result, historical data may offer limited predictive value, and management perceptions may lag developments in the external threat environment [10], [14]. Prior research has documented that internal audit functions frequently struggle to assess cyber risks consistently and to communicate their significance effectively to audit committees [10]. In response, scholars and professional bodies have emphasized the need for more dynamic, data-driven approaches to audit risk assessment [15], [16]. Continuous risk assessment models seek to update risk profiles as new information becomes available, enabling internal audit to respond more quickly to emerging risks. However, the effectiveness of such approaches depends critically on the relevance and interpretability of the information used to inform them.

Notably, internal audit research has largely emphasized internally generated data and organizational controls. The systematic use of external information—particularly structured cybersecurity threat intelligence—remains underdeveloped.

Research Gap: Internal audit literature lacks theoretically grounded explanations of how external cybersecurity threat intelligence enhances risk assessment accuracy, timeliness, and relevance (RQ1).

2.3 AI-Driven Risk Analytics and Continuous Risk Assessment

Advances in artificial intelligence and data analytics have significantly expanded the analytical capabilities available to internal audit functions. AI-driven risk analytics include machine learning–based risk scoring, anomaly detection, predictive modeling, and continuous monitoring of transactional and operational data [15]–[17]. These tools enable internal audit to analyze full populations of data rather than samples and to reassess risk more frequently.

Research suggests that AI-driven analytics can enhance fraud detection, improve audit efficiency, and support continuous assurance [16], [17]. At the same time, studies highlight important limitations. AI models are highly sensitive to data quality, and their outputs may be difficult to interpret or validate as audit evidence [19], [21]. In addition, behavioral research indicates that auditors may exhibit **automation bias**, over-relying on AI-generated outputs and discounting contradictory information [18].

These limitations are particularly salient in cyber risk contexts. Malicious activity is adversarial by nature and often designed to resemble legitimate behavior, generating ambiguous or weak signals. AI models trained primarily on internal historical data may therefore struggle to identify novel or externally driven threats. Despite the growing adoption of AI in internal auditing, existing research rarely examines how AI-driven risk assessment performs when enriched with external threat context.

Research Gap: Prior audit analytics research does not adequately explain how cybersecurity threat intelligence improves the reliability and decision usefulness of AI-driven risk assessment (RQ2).

2.4 Integrating Threat Intelligence into Governance and Audit Decision-Making

Beyond security operations, a growing body of research argues that CTI should be treated as an enterprise information resource rather than a purely technical asset [9], [11]. From this perspective, threat intelligence can inform not only defensive actions but also governance, risk management, and assurance processes.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

However, integrating CTI into internal audit presents organizational and conceptual challenges. Threat intelligence teams and internal audit functions often operate in silos, with different objectives, terminologies, and time horizons. Intelligence products optimized for security operations may lack the abstraction and framing required for audit risk assessment, while auditors may lack the expertise to interpret technical intelligence outputs. Recent standards and guidance emphasize aligning cybersecurity information with enterprise risk management and governance processes [5], [35]–[38]. Yet empirical research examining how CTI is incorporated into audit planning and risk prioritization remains limited.

Research Gap: There is insufficient understanding of how CTI can be effectively integrated into AI-supported internal audit risk assessment and governed to support assurance objectives (RQ3).

2.5 Information Processing and Dynamic Perspectives

Information Processing Theory provides a useful lens for integrating CTI, AI, and internal audit risk assessment. The theory posits that organizational effectiveness depends on the alignment between environmental uncertainty and information processing capacity [29], [30]. Cyber threat environments impose high uncertainty due to rapid change, adversarial intent, and incomplete information.

AI-driven analytics increase processing capacity by enabling large-scale data analysis, while CTI enhances information richness by providing context, meaning, and anticipatory insight. Together, these capabilities enable organizations to process complex cyber risk information more effectively. Importantly, information processing theory emphasizes that such alignment is **dynamic rather than static**, requiring continuous adaptation as environments evolve. While prior studies acknowledge adaptive analytics and evolving threat landscapes, little research has examined **continuous feedback loops** between threat intelligence, AI-driven risk assessment, and audit decision-making over time.

Research Gap: Prior research has not sufficiently theorized the dynamic interaction between CTI and AI-driven risk assessment in internal auditing, particularly with respect to continuous learning and adaptation (RQ4).

3. Theoretical Foundation

3.1 Need for a Theory Addressing Uncertainty and Interpretation

The research questions guiding this study focus on how cybersecurity threat intelligence (CTI) influences AI-driven risk assessment effectiveness in internal auditing, the mechanisms through which this influence occurs, the conditions under which it is strengthened or weakened, and how these relationships evolve over time. Addressing these questions requires a theoretical lens capable of explaining organizational decision-making under conditions of high uncertainty, information asymmetry, and rapid environmental change.

Cyber threat environments are not merely complex; they are adversarial. Threat actors intentionally disguise malicious activity, adapt to defensive measures, and exploit information gaps. Internal audit functions assessing cyber risk must therefore interpret ambiguous signals while maintaining professional judgment and governance credibility. This context makes **Information Processing Theory (IPT)** particularly appropriate.

Information Processing Theory explains how organizations structure information flows and analytical capabilities to cope with uncertainty [29], [30]. It has been widely applied in organizational design and information systems research and offers a strong foundation for examining the joint role of AI-driven analytics and threat intelligence in internal audit risk assessment.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

3.2 Information Processing Theory and Environmental Uncertainty

Information Processing Theory posits that organizational effectiveness depends on the **fit between environmental uncertainty and information processing capacity** [29]. When uncertainty is low, organizations can rely on standardized procedures and limited information. As uncertainty increases, organizations require richer, more timely, and more interpretive information to support decision-making [30].

Cyber risk represents an extreme form of environmental uncertainty. Threats emerge rapidly, originate outside organizational boundaries, and often lack historical precedent. Signals of emerging cyber risk are frequently weak, noisy, and distributed across multiple data sources. Under such conditions, traditional internal audit risk assessment approaches—periodic, retrospective, and internally focused—are poorly aligned with the information processing demands of the environment. From an IPT perspective, this misalignment explains why internal audit functions struggle to assess cyber risks accurately and proactively using conventional methods. It also provides the theoretical basis for adopting advanced analytics and external intelligence inputs.

3.3 AI-Driven Risk Assessment as Information Processing Capacity

AI-driven risk assessment expands internal audit's **information processing capacity** by enabling large-scale, continuous analysis of transactional, operational, and security-related data [15]–[17]. Machine learning models can identify statistical anomalies, generate predictive risk scores, and update assessments in near real time. These capabilities directly address the volume and velocity dimensions of cyber risk information.

However, Information Processing Theory cautions that increased processing capacity alone does not guarantee improved decision quality. When information lacks meaning or context, greater analytical power may simply accelerate the production of ambiguous or misleading outputs. In cyber contexts, AI models trained primarily on internal historical data may fail to recognize novel threats or may normalize malicious behavior that closely resembles legitimate activity.

This limitation is central to **RQ1**, which asks how CTI influences the effectiveness of AI-driven risk assessment. IPT suggests that AI provides capacity, but effectiveness depends on complementary mechanisms that enhance information richness and interpretability.

3.4 Cybersecurity Threat Intelligence as Information Richness

Within the IPT framework, cybersecurity threat intelligence functions as a source of **information richness** rather than processing capacity. CTI transforms raw security data into contextualized knowledge by embedding indicators within narratives about threat actors, tactics, techniques, and campaigns [1], [2]. Strategic and tactical intelligence reduce ambiguity by clarifying which signals are meaningful under current threat conditions, while operational intelligence supports timely prioritization.

For internal audit, this enrichment is critical. Audit risk assessment requires not only detecting anomalies but judging their **governance relevance**. CTI provides external reference points that enable AI systems and auditors to interpret internal signals in light of evolving threat landscapes. For example, an unusual access pattern may be interpreted differently when aligned with intelligence about active credential-based attacks targeting similar organizations. This logic directly supports **RQ2**, which focuses on the mechanisms through which CTI enhances AI-based risk assessment. From an IPT perspective, CTI reduces equivocality and improves signal-to-noise ratios, enabling more consistent and defensible audit judgments.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

3.5 Dynamic Fit, Learning, and Governance

A core insight of Information Processing Theory is that alignment between uncertainty and information processing is **dynamic rather than static** [30]. As environments evolve, organizations must continuously adjust their information processing mechanisms. This perspective aligns closely with both AI systems that learn over time and CTI capabilities that evolve as threat landscapes change.

In the context of this study, dynamic fit is achieved through feedback loops in which CTI informs AI-driven risk assessment, AI outputs shape audit planning and findings, and audit outcomes refine intelligence requirements. Over time, this process can enhance both analytical performance and audit relevance. However, IPT also highlights the risk of maladaptation if feedback loops are poorly governed, leading to reinforcement of biased threat narratives or outdated intelligence. This dynamic perspective underpins **RQ4**, which examines how continuous feedback between CTI and AI affects audit risk assessment performance over time. It also informs **RQ3**, as governance mechanisms determine whether adaptation improves or degrades decision quality.

3.6 Mapping Information Processing Theory to Research Questions

To make the theoretical logic explicit, Table 1 maps key IPT concepts to the research questions addressed in this study.

Table 1: ***Information Processing Theory Constructs and Research Questions***

IPT Concept	Description	Related Research Question(s)
Environmental Uncertainty	Adversarial, rapidly evolving cyber threat landscape	RQ1
Information Processing Capacity	AI-driven risk assessment analytics	RQ1
Information Richness	Cybersecurity threat intelligence	RQ1, RQ2
Equivocality Reduction	Improved interpretation of risk signals	RQ2
Governance and Fit	Oversight of AI and CTI integration	RQ3
Dynamic Adaptation	Continuous learning and feedback loops	RQ4

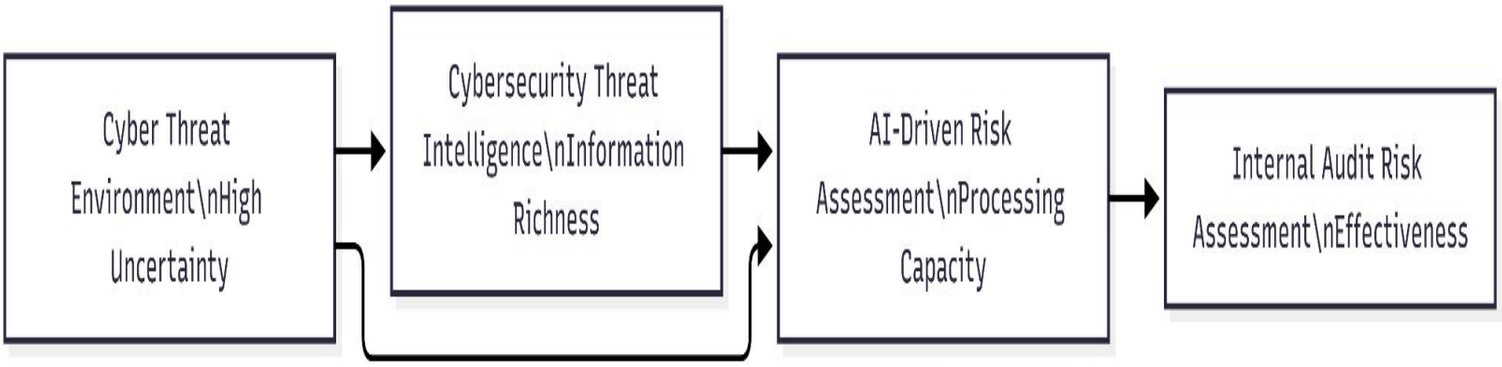
3.7 Theoretical Mechanism Diagram

Figure 1 illustrates how Information Processing Theory explains the joint role of CTI and AI in internal audit risk assessment.

https://doi.org/10.5281/zenodo.18336904

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

Figure 1 .Information Processing Mechanism



4. Conceptual Framework and Hypotheses

4.1 Purpose and Link to Research Questions

To address the research questions articulated in Section 1.7, this section develops a conceptual framework that explains how cybersecurity threat intelligence (CTI) enhances AI-driven risk assessment effectiveness in internal auditing. Specifically, the framework is designed to answer:
(1) how CTI influences AI-driven risk assessment outcomes (RQ1);
(2) through which mechanisms this influence occurs (RQ2);
(3) how AI integration maturity and governance condition these relationships (RQ3); and
(4) how continuous feedback between CTI and AI affects performance over time (RQ4).
Grounded in Information Processing Theory, the framework conceptualizes internal audit risk assessment as an information-intensive decision process operating under conditions of high uncertainty. AI-driven analytics and CTI are treated as complementary capabilities that jointly reduce uncertainty and improve audit judgment.

4.2 Overview of the Conceptual Framework

The proposed framework positions **cybersecurity threat intelligence** as a primary antecedent influencing the effectiveness of **AI-driven risk assessment** in internal auditing. The framework distinguishes between direct effects, mediating mechanisms, moderating conditions, and dynamic feedback effects.

At a high level, CTI enhances AI-driven risk assessment by enriching the informational context in which AI models operate. This enrichment improves the interpretation of risk signals and supports more accurate, timely, and governance-relevant audit judgments. However, the strength of these effects depends on the maturity of AI integration and the presence of appropriate governance mechanisms.

4.3 Construct Definitions

4.3.1 Cybersecurity Threat Intelligence

Cybersecurity threat intelligence is defined as the systematic collection, analysis, validation, and dissemination of actionable information about cyber threats, including threat actors, attack techniques, campaigns, and vulnerabilities [1], [2]. CTI varies in maturity across organizations and may include strategic, tactical, operational, and technical intelligence.

Within the framework, CTI is conceptualized as a source of **information richness** that shapes how AI systems and auditors interpret risk signals.

4.3.2 AI-Driven Risk Assessment in Internal Auditing

AI-driven risk assessment refers to the application of machine learning, predictive analytics, anomaly detection, and continuous monitoring techniques to identify and prioritize risks relevant to internal audit planning and execution [15]–[17]. These systems expand internal

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

audit's information processing capacity by enabling large-scale and continuous analysis of diverse data sources.

AI-driven risk assessment is treated as a **necessary but not sufficient** condition for effective cyber risk assessment, as its outputs depend heavily on the informational context in which models operate.

4.3.3 Internal Audit Risk Assessment Effectiveness

Internal audit risk assessment effectiveness reflects the extent to which risk assessments accurately identify significant risks, detect emerging threats in a timely manner, minimize false positives and false negatives, align with enterprise risk priorities, and support informed oversight by audit committees [10], [14].

Effectiveness is therefore conceptualized as a multidimensional outcome combining analytical performance and governance relevance.

4.4 Direct Effect of Cybersecurity Threat Intelligence (RQ1)

Information Processing Theory suggests that reducing environmental uncertainty improves decision quality. By providing insight into threat actors, attack techniques, and active campaigns, CTI reduces uncertainty surrounding cyber risk exposure and enables AI systems to recalibrate risk scoring and anomaly detection logic.

When AI-driven risk assessment is informed by relevant threat intelligence, risk prioritization is more likely to reflect the external threat landscape rather than historical or internally bounded patterns. This direct effect addresses RQ1.

H1: Cybersecurity threat intelligence is positively associated with the effectiveness of AI-driven risk assessment in internal auditing.

4.5 Mediating Mechanisms: Contextual Enrichment and Signal Quality (RQ2)

The framework proposes that the influence of CTI on AI-driven risk assessment effectiveness is partially mediated by two mechanisms.

Contextual Enrichment refers to the degree to which CTI provides interpretive meaning that clarifies why certain signals matter. By linking internal anomalies to external threat narratives, CTI reduces equivocality and supports more consistent interpretation of AI outputs.

Signal-to-Noise Improvement refers to the reduction of irrelevant or misleading alerts generated by AI systems. CTI enables more effective filtering and prioritization of signals, reducing cognitive overload and alert fatigue.

These mechanisms explain how CTI improves decision usefulness rather than simply increasing information volume, directly addressing RQ2.

H2a: Contextual enrichment mediates the relationship between cybersecurity threat intelligence and AI-driven risk assessment effectiveness.

H2b: Signal-to-noise improvement mediates the relationship between cybersecurity threat intelligence and AI-driven risk assessment effectiveness.

4.6 Moderating Role of AI Integration Maturity and Governance (RQ3)

The framework further recognizes that the benefits of CTI are contingent on how intelligence is integrated into AI systems and governed within the organization. High-quality CTI may fail to enhance risk assessment if it is poorly mapped to audit-relevant risks or ingested into AI models without validation.

AI Integration Maturity moderates the CTI–effectiveness relationship by determining the system's capacity to incorporate evolving intelligence inputs. **Governance mechanisms**, including validation processes, documentation, and human-in-the-loop review, moderate the relationship by ensuring transparency, accountability, and appropriate reliance on AI outputs.

These moderating effects directly address RQ3.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

H3: The positive relationship between cybersecurity threat intelligence and AI-driven risk assessment effectiveness is strengthened by higher levels of AI integration maturity and governance.

4.7 Dynamic and Feedback Effects (RQ4)

Cyber threat environments evolve continuously, and both CTI and AI systems must adapt accordingly. The framework therefore incorporates dynamic feedback effects in which CTI informs AI-driven risk assessment, AI outputs shape audit planning and findings, and audit outcomes refine intelligence requirements.

Over time, this feedback loop can enhance alignment between external threat conditions and internal risk assessment. However, without appropriate governance, feedback may reinforce biased threat narratives or outdated assumptions. This dynamic perspective directly addresses RQ4.

H4: Continuous feedback between cybersecurity threat intelligence and AI-driven risk assessment improves internal audit risk assessment effectiveness over time.

4.8 Conceptual Framework Summary Table

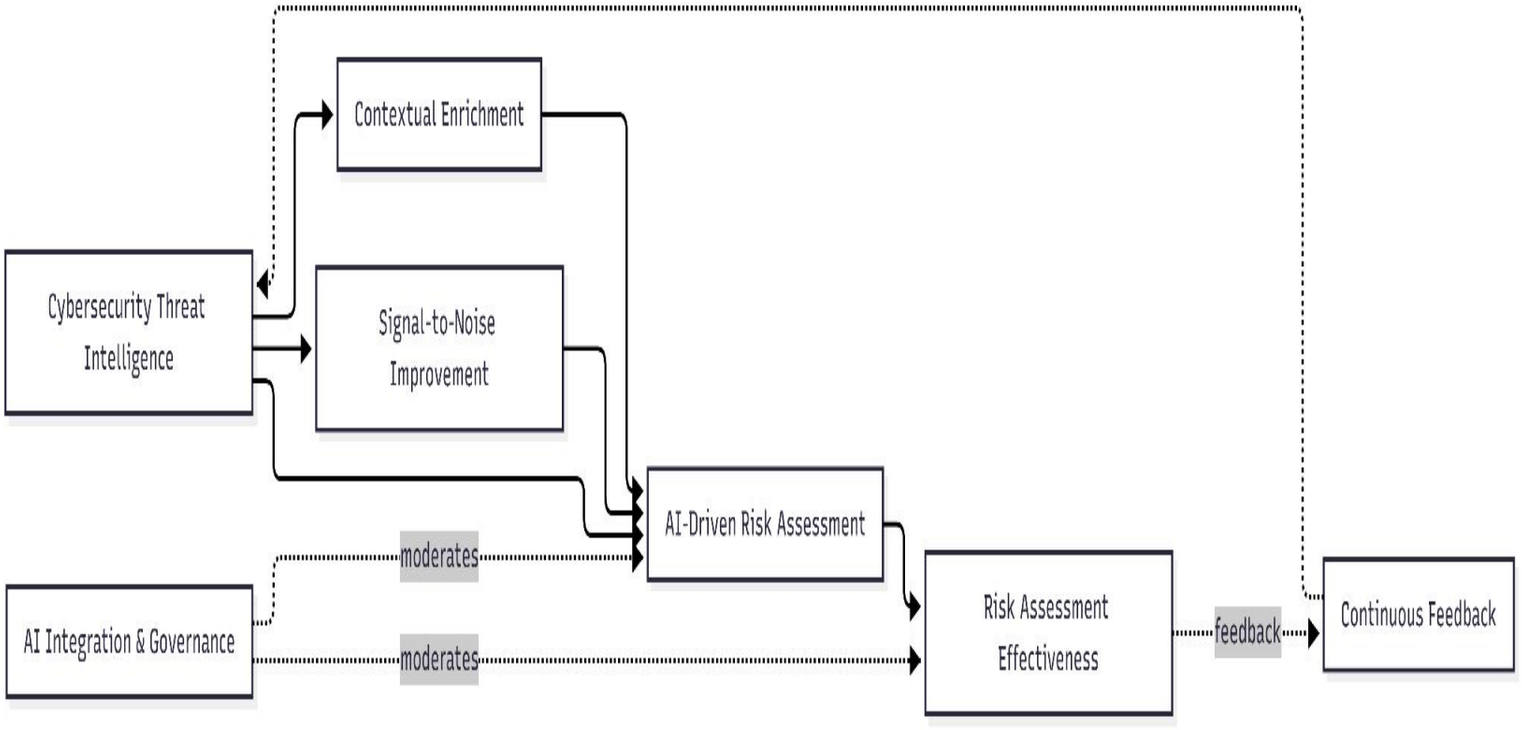
Table 2: ***Summary of Conceptual Framework Components***

Element	Description	Research Question(s)
Cybersecurity Threat Intelligence	External threat context and intelligence capability	RQ1, RQ2
AI-Driven Risk Assessment	Analytical processing capacity	RQ1
Contextual Enrichment	Interpretive mechanism	RQ2
Signal-to-Noise Improvement	Analytical filtering mechanism	RQ2
AI Integration & Governance	Conditioning factors	RQ3
Dynamic Feedback	Continuous learning effects	RQ4
Risk Assessment Effectiveness	Audit outcome	All

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

4.9 Conceptual Research Model Diagram

Figure 2 .Conceptual Research Model



5. Method / Research Design

5.1 Research Design Overview

This study adopts a **theory-driven conceptual research design** with explicit propositions that are empirically testable. Such a design is appropriate given the interdisciplinary nature of the research questions, which span cybersecurity threat intelligence, artificial intelligence, and internal auditing. While empirical data exist in each of these domains independently, integrated datasets capturing CTI maturity, AI-driven risk assessment practices, and internal audit outcomes remain limited and fragmented.

Consistent with prior research in information systems and audit analytics, the objective of this design is to **clarify constructs, specify causal mechanisms, and define boundary conditions** before large-scale empirical testing [15], [20]. The framework is therefore developed with empirical implementation in mind, allowing future studies to test the proposed relationships using survey-based, archival, longitudinal, or mixed-method approaches.

5.2 Alignment of Research Questions and Methodological Approach

The research design is explicitly aligned with the four research questions articulated in Section 1.7.

- **RQ1** examines the direct relationship between cybersecurity threat intelligence and AI-driven risk assessment effectiveness.
- **RQ2** focuses on the mediating mechanisms through which CTI enhances AI-supported audit judgments.
- **RQ3** examines moderating effects related to AI integration maturity and governance.
- **RQ4** addresses dynamic and adaptive effects over time.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

These questions collectively require a design capable of modeling latent constructs, mediation, moderation, and temporal dynamics.

5.3 Conceptual Model Testability and Analytical Techniques

The proposed framework is suitable for empirical testing using **structural equation modeling (SEM)** or **partial least squares SEM (PLS-SEM)**. These techniques are appropriate because they allow simultaneous estimation of multiple relationships among latent constructs, including indirect and interaction effects.

- **Direct effects (RQ1)** can be tested through path coefficients linking CTI to risk assessment effectiveness.
- **Mediation effects (RQ2)** can be assessed using bootstrapped indirect effect analysis.
- **Moderation effects (RQ3)** can be tested through interaction terms or multi-group comparisons based on AI integration maturity or governance levels.
- **Dynamic effects (RQ4)** can be examined using longitudinal SEM, latent growth modeling, or panel data designs where repeated measures are available.

5.4 Construct Operationalization

Table 3: ***Construct Definitions and Illustrative Measurement Items***

Construct	Operational Definition	Illustrative Measurement Items
Cybersecurity Threat Intelligence (CTI)	Maturity and effectiveness of CTI collection, analysis, and use	CTI is timely and relevant; CTI is integrated into risk discussions; Intelligence sources are validated
Contextual Enrichment	Degree to which CTI improves interpretability of risk signals	Threat context clarifies why anomalies matter; External intelligence informs risk interpretation
Signal-to-Noise Improvement	Reduction of irrelevant or misleading AI risk alerts	AI alerts are more precise with CTI; False positives are reduced
AI-Driven Risk Assessment	Extent and sophistication of AI use in audit risk assessment	Predictive risk scoring is used; Continuous monitoring is implemented
AI Integration Maturity	Capability to embed CTI into AI models	AI models adapt to new threat patterns; CTI influences model features
Governance and Oversight	Formal controls over CTI and AI use	AI outputs are reviewed; CTI sources are governed
Risk Assessment Effectiveness	Quality and relevance of audit risk assessments	Emerging risks identified early; Risk prioritization aligns with enterprise risk

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

Survey-based measures can be complemented with objective indicators such as time-to-risk-identification, frequency of CTI-informed audit plan updates, or reductions in false risk alerts.

5.5 Reliability and Validity Considerations

Construct reliability may be assessed using Cronbach's alpha and composite reliability. Convergent validity can be evaluated through average variance extracted (AVE), while discriminant validity may be examined using the Fornell–Larcker criterion and heterotrait–monotrait ratios.

To mitigate **common method bias**, future studies should collect data from multiple respondents, such as internal audit leaders, cybersecurity or CTI managers, and AI governance owners. Where possible, survey responses should be triangulated with archival or system-generated data.

Endogeneity concerns—such as reverse causality between audit effectiveness and CTI investment—can be addressed through longitudinal designs, lagged variables, instrumental variables, or quasi-experimental approaches such as phased implementation of CTI integration.

5.6 Research Design Diagram

Figure 3 summarizes the overall research design logic, linking theory, research questions, constructs, and analytical techniques.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

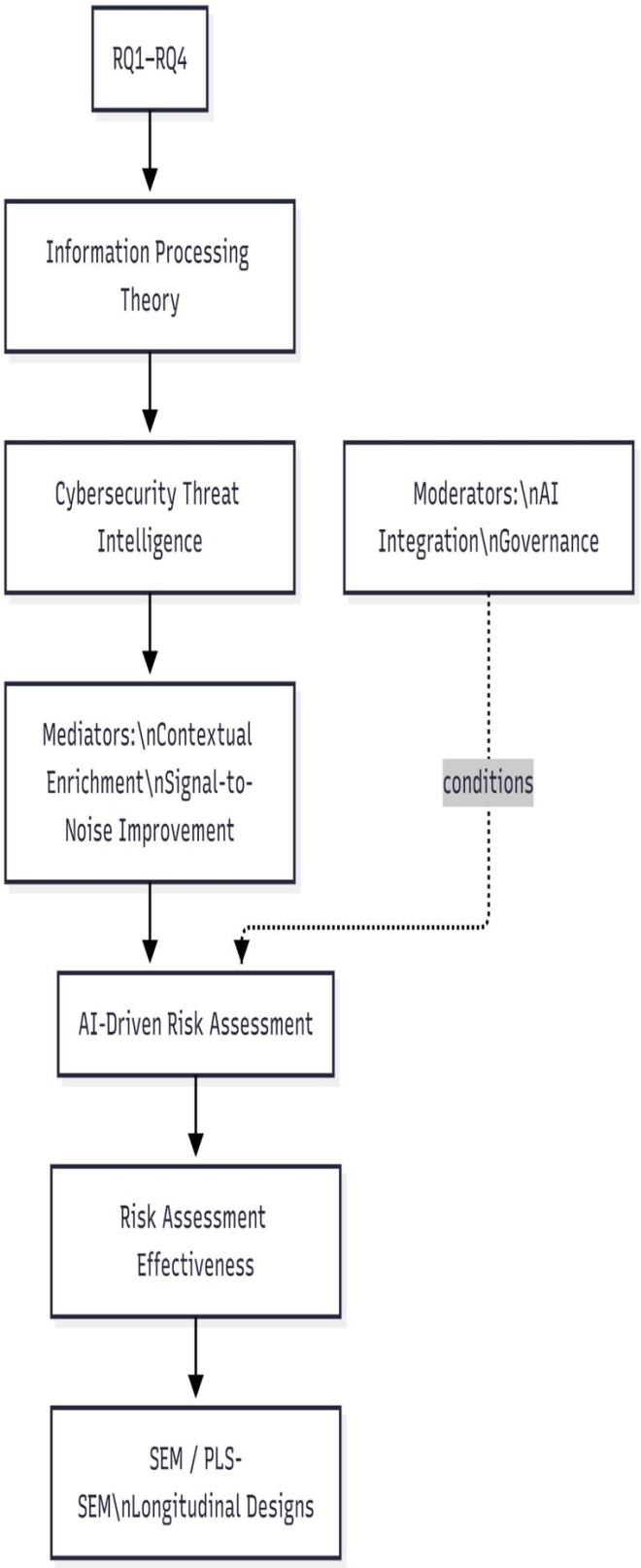


Figure 3. Research Design Overview

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

6. Framework Application and Analytical Results

6.1 Purpose and Nature of the Results

Given the theory-driven conceptual design of this study, this section presents **analytical results in the form of a structured application of the proposed framework** rather than statistical estimates. This approach is consistent with prior conceptual research in information systems and audit analytics, where the objective is to demonstrate explanatory power, boundary conditions, and practical implications of a theoretical model prior to large-scale empirical testing.

The framework is applied across varying levels of cybersecurity threat intelligence maturity to illustrate how CTI shapes AI-driven risk assessment effectiveness in internal auditing. This application directly addresses **RQ1–RQ4** by demonstrating (1) the direct influence of CTI, (2) the mediating mechanisms at work, (3) moderating effects of integration and governance, and (4) dynamic learning over time.

6.2 Cybersecurity Threat Intelligence Maturity Levels

Consistent with prior CTI and capability maturity research, three stylized levels of CTI maturity are considered: **low**, **moderate**, and **high**. These levels do not represent exhaustive categorizations but serve as analytically useful reference points for examining how intelligence capabilities interact with AI-driven risk assessment.

- **Low CTI maturity** is characterized by ad hoc consumption of generic external feeds, limited validation, minimal integration with internal data, and weak governance.
- **Moderate CTI maturity** involves curated intelligence sources, partial contextualization, and episodic integration into risk discussions.
- **High CTI maturity** reflects a fully integrated intelligence capability aligned with organizational risk priorities, supported by validation processes, governance oversight, and continuous feedback.

6.3 CTI Maturity and AI-Driven Risk Assessment Effectiveness

Applying the conceptual framework across these maturity levels reveals systematic differences in AI-driven risk assessment effectiveness.

At **low CTI maturity**, AI-driven risk assessment relies primarily on internal historical data. While AI models may identify anomalies efficiently, they struggle to distinguish emerging cyber threats from benign deviations. As a result, risk assessments exhibit high false-positive rates, delayed recognition of novel threats, and limited relevance for audit planning. In this context, AI expands processing capacity without sufficient informational richness, leading to fragile or misleading outputs.

At **moderate CTI maturity**, AI-driven risk assessment benefits from partial contextual enrichment. Intelligence inputs improve prioritization of certain risk signals and reduce alert fatigue, but integration remains inconsistent. Risk assessments improve in accuracy and timeliness but remain vulnerable to blind spots when intelligence is outdated or weakly governed.

At **high CTI maturity**, AI-driven risk assessment demonstrates substantially higher effectiveness. Contextual enrichment and signal-to-noise improvement are fully realized, enabling anticipatory identification of emerging cyber risks. Risk assessments align more closely with enterprise risk priorities and support more credible communication with audit committees.

6.4 Maturity–Effectiveness Matrix

Table 4 summarizes the relationship between CTI maturity and AI-driven risk assessment effectiveness.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

Table 4: *CTI Maturity and AI-Driven Risk Assessment Outcomes*

CTI Maturity Level	AI Risk Assessment Characteristics	Audit Risk Assessment Effectiveness
Low	AI relies on internal data; limited context	High false positives; delayed detection; low governance relevance
Moderate	Partial CTI integration; episodic enrichment	Improved prioritization; reduced noise; uneven effectiveness
High	Fully integrated CTI; continuous feedback	High accuracy; anticipatory detection; strong audit committee confidence

This matrix illustrates that improvements in CTI maturity correspond to qualitative shifts in audit risk assessment effectiveness rather than linear incremental gains.

6.5 Non-Linear Effects of Threat Intelligence Maturity

A key analytical insight emerging from the framework application is the **non-linear relationship** between CTI maturity and AI-driven risk assessment effectiveness. Initial investments in CTI often yield limited benefits, particularly when intelligence is poorly integrated or weakly governed. However, once CTI reaches a threshold level of relevance, validation, and integration, effectiveness increases sharply.

This threshold effect reflects the interaction between information richness and processing capacity. Below the threshold, CTI introduces additional data without sufficient interpretive value. Beyond the threshold, intelligence meaningfully reduces uncertainty and enhances AI outputs.

This finding directly addresses **RQ1** and **RQ2** and cautions against viewing CTI adoption as a purely incremental improvement.

6.6 Moderating Effects of AI Integration and Governance

The framework application further demonstrates that **AI integration maturity and governance strongly moderate** the CTI–effectiveness relationship. Even at high CTI maturity, weak integration or governance can undermine benefits. Poorly mapped intelligence may bias AI models, while lack of validation may lead to overconfidence in intelligence-informed outputs.

Conversely, strong governance—such as model validation, documentation, and human-in-the-loop review—amplifies the benefits of CTI by ensuring appropriate reliance on AI-supported assessments. These findings directly address **RQ3** and reinforce the importance of governance as an enabling rather than constraining factor.

6.7 Dynamic Feedback and Learning Effects

Finally, the application highlights the importance of **dynamic feedback loops**. At higher maturity levels, audit findings and AI performance metrics inform ongoing intelligence requirements, refining both CTI collection and AI model tuning. Over time, this learning process improves alignment between external threat conditions and internal risk assessment. However, the framework also reveals potential risks. Without governance oversight, feedback loops may reinforce biased threat narratives or outdated assumptions, leading to path

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

dependence. This duality underscores that dynamic learning enhances effectiveness only when governed appropriately, directly addressing **RQ4**.

7. Discussion

7.1 Overview of Key Insights

The purpose of this section is to interpret the analytical results presented in Section 6 in light of the research questions, theoretical foundation, and existing literature. The findings demonstrate that cybersecurity threat intelligence (CTI) plays a critical role in determining whether AI-driven risk assessment enhances or undermines internal audit effectiveness. Importantly, the discussion shows that CTI does not function as a simple additive input to AI systems; rather, its value depends on maturity, integration, governance, and dynamic learning processes.

Across all maturity levels examined, the results consistently indicate that AI-driven risk assessment alone is insufficient for reliable cyber risk evaluation. This finding reinforces the core premise of Information Processing Theory: expanding information processing capacity without corresponding improvements in information richness may increase analytical output but not decision quality.

7.2 Addressing RQ1: How CTI Influences AI-Driven Risk Assessment Effectiveness

The analysis provides a clear answer to **RQ1**. Cybersecurity threat intelligence positively influences the effectiveness of AI-driven risk assessment by reducing environmental uncertainty and enabling more accurate interpretation of analytical outputs. At higher CTI maturity levels, AI-driven risk assessment shifts from reactive pattern recognition to anticipatory risk identification.

This finding extends prior audit analytics research, which has largely emphasized algorithmic capability and internal data availability [15]–[17]. The results suggest that AI effectiveness in internal auditing is contingent on access to externally oriented, forward-looking information. Without CTI, AI-driven risk assessment remains backward-looking and vulnerable to blind spots related to emerging threats.

7.3 Addressing RQ2: Mechanisms of Contextual Enrichment and Signal Quality

The framework application clarifies **how** CTI enhances AI-supported audit judgments, addressing **RQ2**. Two mechanisms—contextual enrichment and signal-to-noise improvement—emerge as central explanatory pathways.

Contextual enrichment allows AI outputs to be interpreted within a broader threat narrative, reducing equivocality and improving judgment consistency. Signal-to-noise improvement reduces alert fatigue and cognitive overload, enabling auditors to focus on risks that matter most for governance and assurance. These mechanisms align with prior research on information overload and decision quality but extend it into the domain of cyber risk and internal auditing.

Crucially, the findings indicate that CTI's value lies not in increasing the quantity of information but in enhancing its **interpretive quality**. This insight helps explain why organizations that indiscriminately ingest external threat feeds often experience diminished analytical performance rather than improvement.

7.4 Addressing RQ3: The Role of Integration and Governance

The discussion of moderating effects directly addresses **RQ3**. The framework application demonstrates that AI integration maturity and governance practices critically shape the CTI–effectiveness relationship. Even high-quality CTI fails to enhance audit risk assessment when intelligence is poorly integrated into AI models or when governance mechanisms are weak.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

This finding contributes to emerging literature on AI governance and model risk management, which emphasizes the importance of validation, transparency, and human oversight [23], [24], [25]. Within internal auditing, governance ensures that CTI-informed AI outputs are treated as decision support rather than authoritative judgments. Strong governance mitigates risks of automation bias, intelligence overfitting, and misalignment with audit objectives.

The results therefore suggest that governance should be viewed as an enabling capability rather than a constraint on innovation.

7.5 Addressing RQ4: Dynamic Learning and Feedback Effects

The framework application provides nuanced insights into **RQ4**, highlighting both the benefits and risks of continuous feedback between CTI and AI-driven risk assessment. At higher maturity levels, feedback loops enhance learning by refining intelligence requirements, improving model calibration, and strengthening alignment between external threats and audit priorities.

However, the analysis also reveals potential failure modes. Without oversight, feedback loops may reinforce biased threat narratives or outdated assumptions, leading to path dependence and reduced sensitivity to novel risks. This duality underscores the importance of governance mechanisms that periodically challenge intelligence assumptions and model behavior. These findings extend Information Processing Theory by illustrating how dynamic fit operates in adversarial environments where learning can both improve and degrade decision quality.

7.6 Comparison with Prior Literature

The findings both align with and extend existing research. Prior studies have documented the benefits of AI in auditing [15]–[17] and the operational value of CTI in cybersecurity [8], [11]. However, few studies have examined their interaction within internal audit risk assessment.

This study advances the literature by demonstrating that CTI and AI are **complementary rather than substitutive** capabilities. It also bridges audit analytics and cybersecurity governance research by positioning CTI as a governance-relevant information resource rather than a purely technical artifact.

7.7 Theoretical Contributions

This study makes three primary theoretical contributions. First, it extends Information Processing Theory to the context of internal audit risk assessment under cyber uncertainty, demonstrating how information richness and processing capacity jointly determine effectiveness. Second, it introduces CTI as a critical antecedent to AI-driven audit analytics, addressing a gap in both audit and cybersecurity research. Third, it theorizes dynamic learning effects and governance conditions that shape long-term outcomes.

7.8 Transition to Practical Implications

While the discussion emphasizes theoretical insights, the findings also have clear practical relevance. The next section translates these insights into actionable guidance for internal audit leaders, cybersecurity teams, and governance bodies, with particular attention to failure modes and control mechanisms.

8. Practical Implications and Risk & Failure Analysis

8.1 Implications for Internal Audit Leadership

The findings of this study have significant implications for Chief Audit Executives (CAEs) and internal audit leaders seeking to deploy AI-driven risk assessment in cyber-relevant domains. The results demonstrate that AI adoption alone does not ensure improved audit outcomes; rather, effectiveness depends on the presence of mature, well-governed cybersecurity threat intelligence capabilities.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

For internal audit leaders, this implies that investments in AI-driven risk analytics should be evaluated in conjunction with the organization's CTI maturity. At low intelligence maturity levels, AI may increase analytical output while simultaneously degrading judgment quality through excessive false positives or misclassification of emerging threats. In such environments, internal audit functions risk providing false assurance or misaligned risk prioritization.

Audit leaders should therefore treat CTI as a **foundational enabler** of AI-driven risk assessment rather than as a peripheral cybersecurity function. This requires active engagement with threat intelligence teams, explicit incorporation of CTI into audit risk assessment processes, and development of audit-specific intelligence requirements aligned with governance objectives.

8.2 Implications for Cybersecurity and Threat Intelligence Functions

For cybersecurity and threat intelligence teams, the findings highlight the importance of tailoring intelligence products for governance and assurance audiences. Intelligence optimized for security operations—often highly technical and time-sensitive—may not translate directly into audit-relevant insight. Without appropriate abstraction and contextual framing, CTI may overwhelm auditors or be misinterpreted.

Threat intelligence functions should therefore collaborate with internal audit to develop **audit-facing intelligence products**, such as threat trend summaries, campaign relevance assessments, and mappings between external threats and internal control domains. This alignment enhances the interpretive value of CTI and supports its effective integration into AI-driven risk assessment models.

8.3 Governance Implications for AI-Driven Risk Assessment

A central practical insight from the study is the critical role of governance in mediating the relationship between CTI and AI-driven risk assessment effectiveness. Governance mechanisms determine whether intelligence-informed AI outputs are used as decision support or treated as authoritative judgments.

Effective governance requires:

- Clear ownership of CTI ingestion and validation
- Documented assumptions embedded in AI risk models
- Human-in-the-loop review of AI-supported risk assessments
- Periodic challenge of intelligence relevance and model behavior

Without these controls, organizations face heightened risks of automation bias, intelligence overfitting, and misalignment between AI outputs and audit objectives.

8.4 Mandatory Risk and Failure Mode Analysis

While CTI enhances AI-driven risk assessment, the framework application reveals several **systematic failure modes** that arise when intelligence quality, integration, or governance is weak. These failure modes are particularly important for practitioners because they often manifest subtly, producing plausible but misleading audit outputs.

Low CTI Maturity Failure Modes

At low CTI maturity levels, intelligence inputs are often generic, outdated, or poorly validated. When such intelligence is ingested into AI systems, models may amplify noise rather than reduce uncertainty. Common failure modes include:

- Misclassification of benign anomalies as high-risk events
- Delayed recognition of emerging threats

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

- Overconfidence in internally derived patterns that no longer reflect the external threat landscape

These failures can result in misplaced audit focus and reduced audit committee confidence.

High CTI Maturity but Weak Governance Failure Modes

Even at high CTI maturity, weak governance introduces distinct risks. Highly contextualized intelligence may bias AI models toward known threat narratives, reducing sensitivity to novel attack vectors. In addition, opaque AI models may obscure how intelligence influences risk scores, undermining auditability.

Failure modes in this category include:

- Automation bias and over-reliance on AI-supported assessments
- Reinforcement of outdated threat assumptions through feedback loops
- Increased vulnerability to adversarial manipulation of intelligence sources

8.5 Failure Modes and Mitigation Controls

Table 5 summarizes key failure modes and corresponding governance and control mechanisms.

Table 5: ***CTI-Informed AI Risk Assessment Failure Modes and Controls***

Failure Mode	Underlying Cause	Potential Impact	Mitigation Controls
Intelligence noise amplification	Low-quality or generic CTI	False positives, alert fatigue	Source validation, relevance scoring
Automation bias	Over-reliance on AI outputs	Misplaced assurance	Human-in-the-loop review
Threat narrative lock-in	Reinforced feedback loops	Blind spots to novel threats	Periodic model and intelligence challenge
Model opacity	Lack of explainability	Reduced auditability	Documentation, explainable AI techniques
Adversarial intelligence manipulation	Unverified external feeds	Distorted risk signals	Feed vetting, cross-source corroboration

8.6 Maturity-Based Roadmap for Adoption

The findings suggest that organizations should adopt AI-driven risk assessment incrementally, aligned with CTI maturity.

- **Low CTI maturity:** Focus on intelligence quality, validation, and relevance before expanding AI use.
- **Moderate CTI maturity:** Pilot CTI-informed AI models in specific audit domains with strong governance oversight.
- **High CTI maturity:** Scale AI-driven risk assessment with continuous feedback and formal governance structures.

This staged approach reduces the risk of premature AI adoption and supports sustainable improvement in audit effectiveness.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

9. Limitations and Future Research

9.1 Conceptual Scope and Empirical Validation

The primary limitation of this study lies in its conceptual nature. While the framework is grounded in established theory and informed by prior empirical research, it has not been empirically tested within a single integrated dataset. As a result, the analytical results presented in Section 6 should be interpreted as theoretically derived expectations rather than statistically validated relationships.

Future research should empirically test the proposed framework using survey-based or archival data collected from internal audit functions, cybersecurity teams, and governance stakeholders. Structural equation modeling or partial least squares approaches would be particularly well suited for testing the direct, mediated, and moderated relationships proposed in this study.

9.2 Measurement and Data Challenges

Operationalizing key constructs such as cybersecurity threat intelligence maturity and AI-driven risk assessment effectiveness presents methodological challenges. CTI quality is inherently multidimensional and context-dependent, varying across industries, threat landscapes, and organizational risk appetites. Similarly, audit risk assessment effectiveness encompasses both analytical accuracy and governance relevance, which may be perceived differently by auditors, management, and audit committees.

Future studies should employ multi-respondent designs and triangulate perceptual measures with objective indicators, such as time to risk identification, changes in audit plan prioritization, or reductions in false risk alerts. Developing standardized CTI maturity and audit analytics measurement instruments represents an important opportunity for future research.

9.3 Generalizability Considerations

The applicability of the framework may vary across organizational contexts. Large, highly regulated organizations may have access to more mature CTI capabilities and governance structures than smaller entities. Similarly, industry-specific threat environments may shape the relevance and value of different forms of threat intelligence.

Future research should examine cross-industry and cross-jurisdictional differences to assess the generalizability of the findings. Comparative studies could explore how regulatory expectations, threat exposure, and organizational scale influence the CTI–AI–audit relationship.

9.4 Dynamic and Longitudinal Research Opportunities

While this study explicitly theorizes dynamic feedback effects, empirical validation of these effects requires longitudinal research designs. Cross-sectional studies may capture static relationships but are insufficient for examining learning, adaptation, and path dependence over time.

Future research should employ longitudinal panel data, case studies, or field experiments to examine how CTI-informed AI risk assessment evolves and how governance interventions influence long-term outcomes. Such studies would provide deeper insight into the sustainability of CTI-enhanced audit analytics.

9.5 Regulatory and Policy-Oriented Research Directions

Finally, the increasing regulatory focus on AI governance and cyber risk management creates opportunities for policy-oriented research. Emerging frameworks and regulations governing

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 4 No. 1 (2026)

AI transparency, accountability, and risk management may significantly shape how CTI is integrated into audit analytics.

Future studies could examine how regulatory requirements influence internal audit adoption of CTI-informed AI tools, the design of governance controls, and audit committee expectations. Integrating regulatory analysis would further strengthen the practical relevance of this research stream.

10. Conclusion

This study set out to examine how cybersecurity threat intelligence enhances AI-driven risk assessment in internal auditing. Motivated by the growing reliance on artificial intelligence for audit planning and the escalating complexity of cyber threats, the article developed a theory-driven framework explaining why and under what conditions CTI improves the accuracy, timeliness, and reliability of AI-supported audit judgments.

Grounded in Information Processing Theory, the study conceptualized internal audit risk assessment as an information-intensive decision process operating under conditions of high uncertainty. The analysis demonstrated that AI-driven analytics and cybersecurity threat intelligence address different dimensions of this challenge: AI expands information processing capacity, while CTI enhances information richness by providing external context, meaning, and anticipatory insight. Importantly, the findings show that these capabilities are complementary rather than substitutive.

By applying the framework across varying levels of CTI maturity, the study highlighted several key insights. First, AI-driven risk assessment without sufficient threat intelligence context is prone to false positives, blind spots, and misleading signals. Second, the benefits of CTI are realized primarily through contextual enrichment and signal-to-noise improvement, rather than through increased data volume alone. Third, governance and integration maturity play a critical moderating role, determining whether CTI-informed AI outputs support sound audit judgment or introduce new sources of bias. Finally, the study emphasized that dynamic learning and feedback can enhance audit effectiveness over time, but only when subject to appropriate oversight.

The article makes several contributions to research and practice. Theoretically, it extends Information Processing Theory to the domain of internal audit risk assessment under cyber uncertainty and introduces cybersecurity threat intelligence as a foundational antecedent to AI-driven audit analytics. Conceptually, it offers a structured framework that integrates CTI, AI capabilities, governance mechanisms, and dynamic adaptation. Practically, it provides internal audit leaders, cybersecurity teams, and governance bodies with actionable insights into how to deploy AI-driven risk assessment responsibly and effectively.

Taken together, the findings underscore a central message: the effectiveness of AI in internal auditing depends not only on algorithmic sophistication but on the quality, relevance, and governance of the information that informs it. As organizations continue to invest in advanced analytics, aligning cybersecurity threat intelligence, artificial intelligence, and audit governance will be essential for delivering credible assurance in an increasingly uncertain digital risk landscape.

References

[1] M. A. Souppaya and K. Scarfone, *Guide to Cyber Threat Information Sharing*, NIST Special Publication 800-150, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2016.

[2] European Union Agency for Cybersecurity (ENISA), *Threat Intelligence: Collecting, Analysing, and Disseminating Information*, ENISA, Athens, Greece, 2020.

[3] MITRE Corporation, *MITRE ATT&CK®: Design and Philosophy*, Bedford, MA, USA, 2021.
[4] Forum of Incident Response and Security Teams (FIRST), *Traffic Light Protocol (TLP): Definitions and Usage*, FIRST, 2016.
[5] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, Gaithersburg, MD, USA, 2018.
[6] J. Springer, J. K. Venkatesh, and S. E. Young, "Measuring the effectiveness of cyber threat intelligence," *Journal of Cybersecurity*, vol. 7, no. 1, pp. 1–17, 2021.
[7] Institute of Internal Auditors (IIA), *International Professional Practices Framework (IPPF)*, Altamonte Springs, FL, USA, 2020.
[8] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, ENISA, Athens, Greece, 2024.
[9] S. Tounsi and A. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, pp. 212–233, 2018.
[10] M. Chatziamanetoglou, N. Pitropakis, S. Papastergiou, and W. J. Buchanan, "Threat intelligence maturity models: A systematic review," *Computers & Security*, vol. 137, 103640, 2025.
[11] R. Santos, J. M. Moura, and P. Cortez, "Context-aware cyber threat intelligence for organizational decision-making," *Decision Support Systems*, vol. 178, 114014, 2025.
[12] M. Husák, M. Čermák, T. Jirsík, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019.
[13] M. Alles and A. Kogan, "Continuous auditing: Theory and application," *Journal of Emerging Technologies in Accounting*, vol. 7, no. 1, pp. 1–16, 2010.
[14] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrating with Strategy and Performance*, COSO, 2017.
[15] G. L. Vasarhelyi, M. A. Alles, and A. Kogan, "Principles of analytic monitoring for continuous assurance," *Journal of Emerging Technologies in Accounting*, vol. 7, no. 1, pp. 1–18, 2010.
[16] J. Jans, M. Alles, and G. Vasarhelyi, "Process mining of event logs in auditing: Opportunities and challenges," *The Accounting Review*, vol. 89, no. 5, pp. 1757–1785, 2014.
[17] R. Debreceny and A. Gray, "Data quality and audit analytics," *Journal of Information Systems*, vol. 31, no. 1, pp. 1–23, 2017.
[18] J. Brown-Liburd, H. Issa, and D. Lombardi, "Behavioral implications of big data's impact on audit judgment," *Accounting Horizons*, vol. 29, no. 2, pp. 451–468, 2015.
[19] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognition*, vol. 84, pp. 317–331, 2018.
[20] M. Eulerich, C. Wagener, and J. Wood, "Evidence on the internal audit function's role in cyber risk management," *Managerial Auditing Journal*, vol. 35, no. 6, pp. 875–903, 2020.
[21] M. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, "The ethics of algorithms: Mapping the debate," *Big Data & Society*, vol. 3, no. 2, pp. 1–21, 2016.
[22] E. Hutchins, "Organizational learning and cyber resilience," *MIS Quarterly Executive*, vol. 18, no. 2, pp. 79–94, 2019.
[23] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST, Gaithersburg, MD, USA, 2023.
[24] International Organization for Standardization, *ISO/IEC 42001: Artificial Intelligence Management Systems*, ISO, Geneva, Switzerland, 2023.

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 4 No. 1 (2026)

[25] European Union, *Regulation (EU) 2024/1684: Artificial Intelligence Act*, Official Journal of the European Union, 2024.
[26] R. McMillan and M. A. Wood, "Sensemaking and intelligence relevance in cyber risk management," *MIS Quarterly*, vol. 43, no. 2, pp. 517–540, 2019.
[27] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed., Thousand Oaks, CA, USA: Sage, 2017.
[28] R. L. Daft and R. H. Lengel, "Organizational information requirements, media richness and structural design," *Management Science*, vol. 32, no. 5, pp. 554–571, 1986.
[29] J. R. Galbraith, *Organization Design*, Reading, MA, USA: Addison-Wesley, 1974.
[30] M. L. Tushman and D. A. Nadler, "Information processing as an integrating concept in organizational design," *Academy of Management Review*, vol. 3, no. 3, pp. 613–624, 1978.
[31] W. J. Orlikowski, "The duality of technology: Rethinking the concept of technology in organizations," *Organization Science*, vol. 3, no. 3, pp. 398–427, 1992.
[32] N. Papernot et al., "Practical black-box attacks against machine learning," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, 2017, pp. 506–519.
[33] Basel Committee on Banking Supervision, *Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239)*, Bank for International Settlements, Basel, Switzerland, 2013.
[34] G. L. Vasarhelyi, K. Krahel, and M. A. Alles, "Continuous auditing," *Accounting Horizons*, vol. 29, no. 1, pp. 1–19, 2015.
[35] National Institute of Standards and Technology, *NISTIR 8286A: Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*, NIST, 2019.
[36] National Institute of Standards and Technology, *NISTIR 8286B: Prioritizing Cybersecurity Risk for Enterprise Risk Management*, NIST, 2019.
[37] National Institute of Standards and Technology, *NISTIR 8286C: Staging Cybersecurity Risks for Enterprise Risk Management*, NIST, 2020.
[38] M. Alles, G. Brennan, A. Kogan, and M. Vasarhelyi, "Continuous risk monitoring," *Journal of Emerging Technologies in Accounting*, vol. 15, no. 2, pp. 1–20, 2018.
[39] A. Rai, "Explainable AI: From black box to glass box," *Journal of the Academy of Marketing Science*, vol. 48, no. 1, pp. 137–141, 2020.
[40] S. Gregor and D. Jones, "The anatomy of a design theory," *Journal of the Association for Information Systems*, vol. 8, no. 5, pp. 312–335, 2007.