applied sciences

MDPI

Article

An Anti-Sheriff Cybersecurity Audit Model: From Compliance Checklists to Intelligence-Supported Cyber Risk Auditing

Ndaedzo Rananga * and H. S. Venter

Faculty of Engineering, Built Environment and Information Technology, Department of Computer Science, University of Pretoria, Pretoria 0002, South Africa; hventer@cs.up.ac.za

* Correspondence: u11329892@tuks.co.za

Abstract

The increasing adoption of data-driven techniques in cybersecurity has introduced new opportunities to enhance detection, response, and automation capabilities within the cybersecurity ecosystem; however, cybersecurity auditing remains constrained by traditional compliance-oriented approaches that rely profoundly on binary, checklist-based evaluations. Such approaches often reinforce a policing or "sheriff-style" perception of auditing, emphasizing enforcement rather than enablement, risk insight, and organizational improvement. Of primary concern is that the "sheriff-style" cybersecurity audit approach often fails to accurately portray the true state of an organization's cybersecurity posture, often providing a misleading sense of assurance based solely on formal compliance and controls existence. This study proposes an Anti-Sheriff Cybersecurity Audit Model, that moves beyond cybersecurity control checklists, by integrating intelligence-informed risk assessments with structured human judgment to support a more robust, adaptive, and risk-oriented auditing process. Grounded in design science research (DSR), the proposed approach combines conventional binary compliance verification with intelligence-derived risk indicators and governance-based maturity assessments to evaluate cybersecurity controls across technical, operational, and organizational dimensions. The approach aligns with established standards and frameworks, including International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001, the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS) benchmarks, while extending their application beyond static compliance validation. A fictional case study is used to demonstrate the model's applicability and to illustrate how hybrid scoring can reveal residual risk not captured by conventional cybersecurity audits. The findings indicate that combining intelligence-informed analytics with structured human judgment enhances audit depth, interpretability, and business relevance. The proposed approach, therefore, provides a foundation for evolving cybersecurity auditing from just periodic compliance assessments, toward a continuous, risk-informed, and governance-aligned assurance system.

Keywords: cybersecurity risk-based auditing; intelligence-supported audit; human judgment in auditing; control effectiveness; security maturity models; defense-in-depth; continuous assurance; audit analytics

Academic Editor: Hiroaki Kikuchi

Received: 20 January 2026
Revised: 11 February 2026
Accepted: 13 February 2026
Published: 27 February 2026

1. Introduction

It is undeniably true that digital platforms such as web services have become an epicenter of our lives [1]. As articulated by Ndaedzo and Venter [2], among the several

factors directly influencing the exponential adoption of modern technologies, mobility remains one of the most significant. Notably, the surge of technological adoption and digital transformation was also observed during and after the COVID-19 pandemic [3]. The emergence of high-speed technologies, such as 5G, and the proliferation of Internet of Things (IoT) devices have inevitably intensified society's reliance on and appreciation for seamless digital communication [4]. No industry is exempt from the wave of digital transformation, with smart cities in urban planning and development serving as a typical example of how digital technologies are increasingly shaping and influencing nearly every aspect of modern society [5]. Network configurations are now designed to enable users to access computing resources anytime, anywhere, and from almost any device [2]. This ease of access to networking resources has contributed directly to the accelerated adoption of modern technological advancements by end users and organizations.

Concurrently, data-driven and intelligent technologies have moved beyond theoretical exploration and are becoming a central focus of the modern information and communication technology (ICT) landscape [6]. As a result of technologies such as IoT, Artificial Intelligence of Things (AIoT) [7], mobile cloud computing, and ubiquitous computing, the contemporary ICT environment is increasingly saturated with interconnected devices, influencing activities that range from everyday routines to professional work practices. These interconnections also extend to the supply-chain ecosystem and third parties for seamless interactions [8]. While these advancements warrant recognition and appreciation, they are also inevitably associated with increasingly complex and sophisticated cyber threats [9]. Growing concerns have arisen regarding both the nature of modern cyber threats and their frequency [10]. Cybercrimes are becoming stealth and sophisticated [11], moving from a mere computer crime to national threats that have the potential to result in cyber warfare between nations. The financial impact of cybersecurity threats can be estimated at up to trillions of USD at a global level [12], and a single breach can cause up to $3.86 million loss, according to IBM security reports [13]. Notably, no single cybersecurity capability can be considered a universal solution to the increasingly complex and evolving threat landscape; hence, there is a need for an integrated, evolving stance. As demonstrated by Yaker et al. [4], certain modern technologies, such as 5G, IoT, and industry 4.0 smart factories, require novel cybersecurity approaches to mitigate the threats associated with their adoption, since a wide range of cyber threats behave differently in different conditions [14].

Organizations and researchers continue to enhance cybersecurity controls through a range of innovations and applications; however, the nature of cybersecurity necessitates that such controls undergo continuous improvement and evaluation to ensure their effectiveness and adequacy. To facilitate ongoing evaluation of cybersecurity controls, organizations commonly adopt the practice of cybersecurity auditing. This process is closely related to traditional forms of auditing, including information systems (IS) auditing and financial auditing. It is intended to test the resilience of cybersecurity controls and to assess whether they comply with organizationally defined policies or internationally recognized standards, such as ISO, CIS, and NIST [15]; however, with the rise in increasingly sophisticated and evolving cyber threats, conventional cybersecurity audit approaches are becoming less effective in identifying and mitigating the actual risks organizations encounter. Traditionally, cybersecurity audits rely extensively on binary compliance and noncompliance evaluations. To ensure that cybersecurity auditing remains relevant and effective, there is a need to rejuvenate conventional auditing methodologies so they respond more effectively to modern security threats, as traditional audit approaches are increasingly showing insufficiency.

Of particular concern is the prevailing perception that cybersecurity auditing should be approached as policing, hence, referred to as a "sheriff-style" approach. This methodology

places more significance on enforcing compliance with predefined standards or policies enacted through checklists and periodic assessments. In practice, these methods tend to prioritize control evaluation, with limited emphasis on human judgment and contextual insight that could support organizations in continuously improving their cybersecurity posture. As a result, such approaches often fall short, and stakeholders may intentionally mislead audit processes by withholding critical information to avoid unfavorable findings.

Within this context, there is an increasing interest in leveraging intelligence-informed techniques—such as risk indicators derived from threat intelligence, vulnerability exploitation likelihood, and contextual analytics—to enhance cybersecurity auditing. Organizations, however, remain cautious about adopting highly automated or opaque solutions, particularly where human judgment, accountability, and governance considerations are insufficiently addressed. The problem motivating the present study is therefore twofold. First, cybersecurity auditing is frequently perceived as a "sheriff-style" compliance exercise rather than a risk-oriented assurance process. Second, existing approaches often fail to balance intelligence-derived insights with structured human judgment, limiting their practical value for governance-aligned decision-making.

In response to these challenges, this study proposes an Anti-Sheriff Cybersecurity Audit Model that moves beyond control checklists toward intelligence-supported cyber-risk auditing. The model integrates conventional compliance verification with intelligence-informed risk indicators and governance-based maturity assessment, while explicitly retaining human judgment as a central component of the audit process. The importance of human-in-the-loop cannot be overlooked [16], as such models should aim to enhance audit depth, interpretability, and relevance by supporting more adaptive and risk-informed assurance whilst engaging human insights.

At this point, the authors have presented the problem statement, and a high-level overview of the research objective is also presented. To further expand on the problem statement and to emphasize the importance of undertaking this study, the next section presents a standalone discussion of the study motivation, the research objectives, and the anticipated outcomes. The importance of presenting a standalone study motivation that entails the study objective was emphasized by Ali [17] and Alenezi et al. [18].

2. Study Motivation and Contribution

As already stated in the introductory section, it is evident that modern technological advancements are associated with a wide range of opportunities. Notably, no area seems to be exempted to the use and the wave of modern technologies such as AI. As noted in Mohammad et al. [19], AI is also being appreciated in areas such as financial ratio analysis. Further to that, as appreciated in the present study, ML and AI are also being incorporated within the broader IT audit landscape, as was demonstrated in the study done by Zastempowsk et al. [20]. Invertibly so, just like any other technological advancements or a mere change within the ICT fraternity, there is a wide range of challenges that are associated with the modern technological advancements. Modern technologies, particularly AI, have gained increasing recognition even in the less developed countries such as Sub-Saharan Africa, as put forth by Muringani et al. [21]. While these technologies offer substantial opportunities to enhance cybersecurity capabilities, cybersecurity auditing has largely remained grounded in traditional, compliance-driven practices. There is a growing need to adopt intelligence-driven approaches and data-driven approaches [6] that enable cybersecurity controls to be scrutinized through sound auditing methods. In order to respond to the ever evolving cyberthreats, the modern cybersecurity audit approach should move beyond binary, checklist-based assessments focused solely on the existence of controls. The cybersecurity audit should incorporate real-world effectiveness,

contextual relevance, or residual risk exposure, particularly looking at the complex and sophisticated cyber threats. As articulated in the introduction, the primary shortcoming of the binary check "sheriff-style" approach is its tendency to reinforce a policing mindset that prioritizes enforcement over insight, learning, and organizational improvement, often resulting in a misleading sense of assurance where formal compliance is equated with actual security adequacy.

This study is, therefore, motivated by the need to bridge current cybersecurity gaps by re-conceptualizing cybersecurity auditing as a risk-informed, intelligence-supported, and governance-aligned assurance activity. Rather than replacing auditors with automated systems, the study argues for a balanced, hybrid approach that augments conventional compliance checks with intelligence-supported risk indicators and structured human judgment. The audit ecosystem is sensitive by nature, and as such, due diligence becomes a key to a sound outcome of the whole audit. In a quest to address shortcomings from the current audit approach, the present study demonstrated that the underutilization of external threat intelligence can mislead the audit outcome and should be addressed as a matter of urgency. In order to address the defined problem that motivated the current study, the proposed Anti-Sheriff Cybersecurity Audit Model is essential to advance cybersecurity auditing.

The first essential step to achieve the objective of the current study is to acknowledge that a wide range of controls, standards, and frameworks already exist to address cybersecurity challenges. However, due to the increasing sophistication, scale, and innovation of modern cyber threats, conventional approaches that focus primarily on confirming the existence of controls are becoming less effective. To date, the literature offers limited approaches that move beyond control existence toward evaluating contextual effectiveness and risk relevance. Consequently, there is a pressing need to undertake this type of study. Bearing this in mind, the objectives of the present study are summarized as follows:

- Systematically examine the limitations of traditional cybersecurity auditing approaches and why they are becoming less effective in the modern era of complex cybersecurity threats.
- Investigate the role of external intelligence sources, including Open-Source Intelligence (OSINT) and exploit-probability metrics such as Exploit Prediction Scoring System (EPSS), in enabling risk-based, intelligence-informed cybersecurity audit scoping to extend beyond a mere confirmation of the existence of a cybersecurity control.
- Propose a sound cybersecurity auditing model that is grounded on the hybrid approaches of governance-aware and intelligence-driven risk assessments.
- Demonstrate, using a defined fictional case scenario, how the proposed model can support a transition from periodic audits to continuous cybersecurity assurance.

To approach this problem and to achieve the goal of the study, the remainder of the study is organized as follows: Section 3 presents background concepts relevant to the study; Section 4 outlines the research methodology adopted; Section 5 introduces the study's main contribution by outlining the proposed model; Section 6 discusses study limitations and future research directions; Section 7 concludes the paper, followed by a disclaimer regarding using certain resources in Section 8.

3. Background

As noted by Craigen et al. [22], much of the ICT terminology established in the literature is frequently subjective and occasionally lacks sufficient precision; therefore, it is necessary to provide explicit definitions for key terms used throughout this study, as outlined in the subsequent points. It is essential to note that the definitions in the existing

literature are largely aligned; however, without being explicitly constrained to the scope of this study, they tend to remain broad and, in some instances, ambiguous.

3.1. Cybersecurity

Diverse authors define cybersecurity concepts in varying ways; nevertheless, these descriptions generally align with established principles. Corporations, likewise, define and classify, for instance, assets in distinct ways, depending on criteria specific to their business needs. Cybersecurity, in the present context, focuses on protecting digital assets, including data, information, systems, and services, from potential harm arising from successful negative cyber incidents. As cybercriminals become more innovative and introduce increasingly complex and sophisticated threats, such as advanced persistent threats (APTs), which are difficult to detect, there is an increasing need to strengthen cybersecurity controls [23]. Cybersecurity, therefore, involves systematic assessment and testing of an organization's internal controls, including policies, configurations, and procedures, to determine the resilience of these controls against potential cyber threats [24].

Cooke [25] asserts that cybersecurity broadly encompasses policies, technologies, and personnel that protect corporate network infrastructure from potential cyber threats, detect such threats, and remediate them within a reasonable recovery time objective (RTO) [1]. Diverse authors define cybersecurity in different ways, depending on their areas of work and study objectives; nevertheless, these definitions consistently focus on cybersecurity as ensuring the confidentiality, integrity, and availability (CIA) of valuable digital assets. According to the NIST, cybersecurity can be defined as the:

> *'Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation'*. [26].

Craigen et al. [22] reviewed existing cybersecurity definitions to formulate a definition that summarizes those from multidisciplinary groups. They define cybersecurity as:

> *'The organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights'*. [22].

Cybersecurity auditing shares a symbiotic relationship with other traditional forms of auditing, including performance audits, fraud audits, financial audits, and IS audits. Among these, the IS audit bears the closest resemblance and relevance to cybersecurity auditing in this study. For this reason, before examining the background and context of cybersecurity auditing, it is necessary to establish a clear common understanding of IS auditing, as presented in the subsequent section.

3.2. Information System Audit

According to the Information Systems Audit and Control Association (ISACA), the term audit refers to the formal inspection and verification used to determine whether a standard or set of guidelines is followed, whether records are accurate, and whether efficiency and effectiveness targets are met [27]. Auditors conduct auditing to assess predefined controls or to evaluate controls against defined risks [27]. Auditing relies on several critical components: it must remain process-oriented, independent, and objective to determine the extent to which internal controls counter environmental risks [3].

In financial auditing, auditors aim to ensure the integrity of financial transactions while preventing fraudulent activities or human error that can result in material irregularities (MI). Similarly, the IS audit process is to ensure that the integrity of systems, storage, processing,

and transmission of valuable information is maintained, thereby guaranteeing that stored information remains intact and trustworthy. In its simplest form, IS auditing can be defined as a formal, independent, and objective examination of an organization's IT infrastructure to determine whether the activities (for example, procedures and controls) involved in collecting, processing, storing, distributing, and using information, comply with guidelines, hence, safeguard assets, maintain data integrity, and operate effectively and efficiently to achieve the organization's business objectives [27]. In essence, each organization that adopts the advancement of technological tools, one way or the other, should be subjected to an IS audit to ensure continuous asset protection [28]. As also articulated by Al-dhaqm et al. [29], it is a must for organizations to implement sound cybersecurity measures to protect valuable assets.

Cybersecurity vulnerability assessment and cybersecurity auditing remain closely related procedures, yet they differ fundamentally in scope, methodology, and purpose. Both contribute to an organization's overall cybersecurity status; however, their objectives serve distinct functions: one focuses on technical assessment, while the other focuses on governance. For this study, this comparison remains of limited relevance and is not expanded further. The subsequent section, therefore, presents the concept of cybersecurity auditing, which supports the proposed model.

3.3. Cybersecurity Auditing

The ISACA introduced the concept of cybersecurity auditing at an elevated level through the official Certified Information Systems Auditor (CISA) manual published in 2015, which serves as a central authority in IS auditing. The CISA Review Manual, 26th Edition (2022), subsequently integrated the concept of cybersecurity auditing more comprehensively into auditing practice. This progression indicates that cybersecurity auditing, in its entirety, remains a relatively new concept that has only recently acquired traction within the auditing landscape.

Cybersecurity auditing constitutes a specialized process for assessing IT infrastructure against an organization's security policies, controls, governance arrangements, and compliance with defined standards, whether internal or international. The distinction between conventional vulnerability assessment and cybersecurity auditing remains subtle, with differences primarily evident in methodology, objectives, scope, and the anticipated outcomes of the process. According to Al-Matari [28], contemporary approaches to cybersecurity auditing require extensive examination of available technologies, methodologies, and processes. One notable development in efforts to strengthen cybersecurity capabilities is the adoption of intelligence in the notion. The subsection below presents selected applications of intelligence in cybersecurity.

3.4. Intelligence in Cybersecurity

Cybersecurity researchers increasingly apply intelligence-supported techniques to strengthen cybersecurity controls and counter the evolving, complex, and sophisticated nature of cyber threats. Researchers also recognize intelligence-supported techniques as a potentially powerful tool for confronting complex and sophisticated cybersecurity challenges [23]. Common applications of these approaches in cybersecurity include real-time detection, automated incident response, predictive analytics, and vulnerability management [16]. In practice, intelligence in cybersecurity is often operationalized through analytical methods that process large volumes of heterogeneous security data, including system logs, network telemetry, vulnerability disclosures, and open-source intelligence (OSINT). Examples include identifying abnormal behavior patterns, estimating the likelihood of vulnerability exploitation, correlating alerts across security controls, and supporting priori-

tization of remediation activities. Such techniques aim to augment human decision-making by providing probabilistic risk indicators and contextual insights, rather than deterministic or fully autonomous decisions. Mohawesh et al. [6] have also focused on the need for more data-driven risk assessment, especially these days in the era of Generative artificial intelligence (GenAI).

There is a growing adoption of intelligence-supported cybersecurity approaches; despite this, there still exists a wide range of limitations associated with these approaches. Firstly, within the cybersecurity fraternity, there are questions around interpretability, explainability, and audit transparency that are not yet fully addressed. Particularly where complex analytical models or opaque scoring mechanisms are used, the auditee (organizations being audited) might raise a lot of questions regarding the trustworthiness of the whole process. The other challenge is that cybersecurity intelligence often suffers from fragmented data sources, inconsistent data quality, and limited real-time availability, which can reduce the reliability and timeliness of derived insights. Another main concern, defined already, is that many intelligence-based approaches focus primarily on technical detection or response effectiveness, with limited consideration of governance, compliance alignment, and audit accountability, which are key aspects within the auditing landscape.

If these challenges are not addressed as a matter of urgency, auditors will frequently revert to conventional binary, checklist-based evaluations that verify control existence but fail to capture contextual effectiveness or residual risk. The present study builds on these observations by positioning intelligence as a supporting mechanism within cybersecurity auditing rather than as a replacement for human expertise or governance processes. The proposed Anti-Sheriff Cybersecurity Audit Model leverages intelligence-derived risk indicators—such as exploit likelihood and public exploit maturity—to enhance traditional compliance assessments, while at the same time, explicitly retaining structured human judgment to ensure interpretability, accountability, and alignment with audit objectives. This point will be further expanded after the methodology.

The preceding sections introduced the background, key terminologies used throughout the study, and motivational challenges that influenced the current study. Before presenting the proposed Anti-Sheriff model, the next section presents the research methodology adopted in the present study. This ensures that the model development follows a systematic approach and can be validated through scientific and empirical assessments, thereby supporting credible and replicable outcomes. It is essential to note that, as this study is not a standalone systematic review, the authors did not adopt formal systematic review methodologies such as Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA). Instead, the identified gaps have been synthesized and summarized within the study motivation section. Given the exploratory and design-oriented nature of the current research, the Design Science Research (DSR) approach is deemed more appropriate and is therefore adopted, as presented in the following section.

4. Methodology

As was evident from Al-dhaqm et al. [29], defining research methodology is essential for developing a sound solution to address a defined problem statement. The study employed the DSR methodology. The DSR methodology represents a widely used scientific approach supporting the development and evaluation of innovative artifacts, including models, methods, and frameworks. As succinctly explained by Vom Brocke et al. [30], DSR enhances technology, improves processes, and advances scientific knowledge through the creation of innovative artifacts that solve problems and improve day-to-day operations.

As illustrated in Figure 1, the DSR methodology comprises six research steps: problem identification and motivation, solution objectives definition, design and development,

demonstration, evaluation, and communication. Venable et al. [31] explicate that these steps support research paradigms that produce innovative solutions to practical problems through developing scientifically sound solutions to modern and advanced problems faced by communities at large. In the present study, the authors apply the DSR methodology to establish the foundation for the proposed Anti-Sheriff Model. As presented in the introductory section, the study examines the persistent perception of cybersecurity auditing as a tick-box or binary compliance exercise, particularly in the modern technological era, including AI-enabled cybersecurity threats. With the rise in modern cybersecurity threats, such as third-party risks associated with platforms, such as cloud platforms [8], there is a need for a sounder, systematic approach to address these challenges.

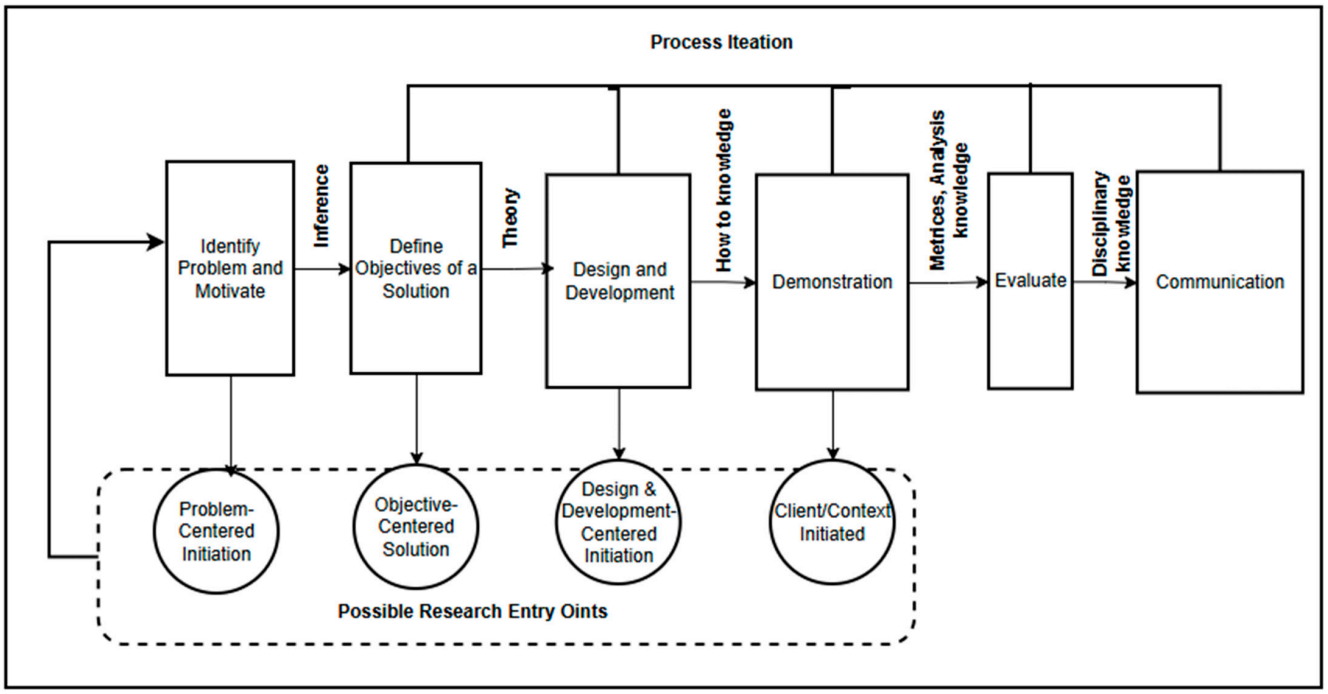

Figure 1. The design science research (DSR) methodology process model was applied in the present study. (Adapted from Vom Brocke et al. [30]).

The adoption of DSR grounds the Anti-Sheriff Cybersecurity Audit Model in real-world auditing challenges, including the need for empirical, intelligence-driven solutions that extend beyond traditional compliance checklists. This approach also safeguards the scientific rigor of the model by integrating established auditing standards, cybersecurity frameworks, and empirical validation techniques to support the proposed solution. The cruciality of appreciating standards such as NIST and ISO within the risk assessment ecosystem has been demonstrated in a study by Pinto et al. [8]. In addition, researchers are broadly and consistently emphasizing the cruciality of aligning proposed solutions with widely recognized standards, which Sulistyowati et al. [11] concur with.

The previous section presented the iterative process of identifying problems through environmental analysis. This section provides an overview of how the DSR processes were applied in the present study, before a delineation of the remainder of the study. Table 1 summarizes the methodology for the proposed model, using the design science research DSR, specifically, the Anti-Sheriff Cybersecurity Audit Model.

Table 1. Methodology summary using the DSR for the Anti-Sheriff Cybersecurity Audit Model.

DRS Model Steps (Adopted from [30])	Description (What the Step Means) [30]	Application in the Present Study	Expected Outcome
1. Problem Identification & Motivation	This step provides the foundational motivation for the study by identifying the problem. In addition, the process identifies. This step presents the gaps and the reasons why a need exists to resolve those gaps through the proposed solution.	In the present study, the authors identify an over-reliance on binary, checklist-based cybersecurity audits. Such audits often fail to assess cybersecurity risk in relation to business objectives, leading stakeholders to perceive auditing as a policing or compliance exercise rather than a value-adding, risk-oriented process.	To define the cybersecurity audit problem.
2. Define the Objectives of a Solution	This step narrows the study objective toward specific end goals and the new artifacts the study aims to present to the body of knowledge.	The study aims to develop a layered cybersecurity audit model that extends beyond binary checks by integrating intelligence-supported risk indicators and structured human judgment to improve audit relevance, interpretability, and business alignment.	Defined research objectives and target framework capabilities.
3. Design & Development	This is the first main contribution of the study, in which the proposed model is presented through a conceptual model and/or a systematic framework.	The Anti-Sheriff Cybersecurity Audit Model is designed as a three-layer structure consisting of (i) binary compliance verification, (ii) intelligence-supported analytical assessment, and (iii) human judgment and governance interpretation.	A functional Anti-Sheriff Cybersecurity Audit Model.
4. Demonstration	The practical applicability of a solution should be applied through a scientific approach, such as experiments. This step demonstrates the applicability of the solution in practice.	The proposed model is applied to a fictional SME case study (Nany FinTrust MicroBank) to demonstrate how layered auditing produces governance-aligned and risk-informed audit insights beyond traditional compliance outcomes.	Demonstrate the applicability of the model using a well-structured fictional scenario.
5. Evaluation	This step ensures that gaps in the proposed solution are identified and resolved. The step also guards against limitations of the proposed solution.	The model is evaluated through quantitative scoring comparisons (binary-only vs. layered assessment) and qualitative reasoning to assess interpretability, governance alignment, and audit usefulness. Limitations and improvement areas are discussed.	Evaluate model effectiveness and identify refinement opportunities.
6. Communication	Finally, the output of the study is made available to the intended society.	The study is documented as a research contribution and prepared for dissemination through peer-reviewed journal publications and academic conferences.	Communicate and publish research outputs.

The preceding Table 1 details the background and the methodology employed in this study. The next section introduces the model, beginning with a high-level representation and subsequently expanding its procedures through a detailed representation.

5. Model Presentation

The proposed model serves as a foundational baseline for enhancing cybersecurity auditing through intelligence-supported risk assessment, while ensuring balanced consideration of three key pillars: technical, compliance, and operational/governance dimensions. As its name suggests, the Anti-Sheriff Cybersecurity Model seeks to transition the prevailing perception of cybersecurity by transforming from a policing or enforcement-driven exercise toward a more risk-informed, adaptive, and enablement-oriented approach. In doing so, the model explicitly incorporates human-centric considerations, including ethics, professional judgment, explainability, transparency, and public trust; these are essential for credible and accountable audit outcomes. Explainability and transparency are among the key determining factors for the adoption of modern technologies such as AI [32]. The proposed model is presented next, starting with a high-level representation before diving into finer details of the model.

5.1. High-Level Anti-Sheriff Cybersecurity Audit Model

The proposed model entails three core components: test 1 (Conventional Cybersecurity Binary Check Layer); test 2 (Intelligence-Supported Risk Indicators, that is analytical layer), and test 3 (Human Judgment and Governance Interpretation, that is decision layer). These layers are built in such a way that they promote integration of different testing procedures for a sound cybersecurity audit outcome, as graphically represented in Figure 2. The model is a layered audit architecture designed to address the limitations of conventional checklist-based cybersecurity auditing. As already alluded to, traditional cybersecurity audits often emphasize binary compliance verification, reinforcing a policing or enforcement-oriented ("Sheriff-style") mindset that prioritizes control existence over control effectiveness, resilience, and governance relevance. A detailed explanation of each component of the model is presented after the graphical representation.

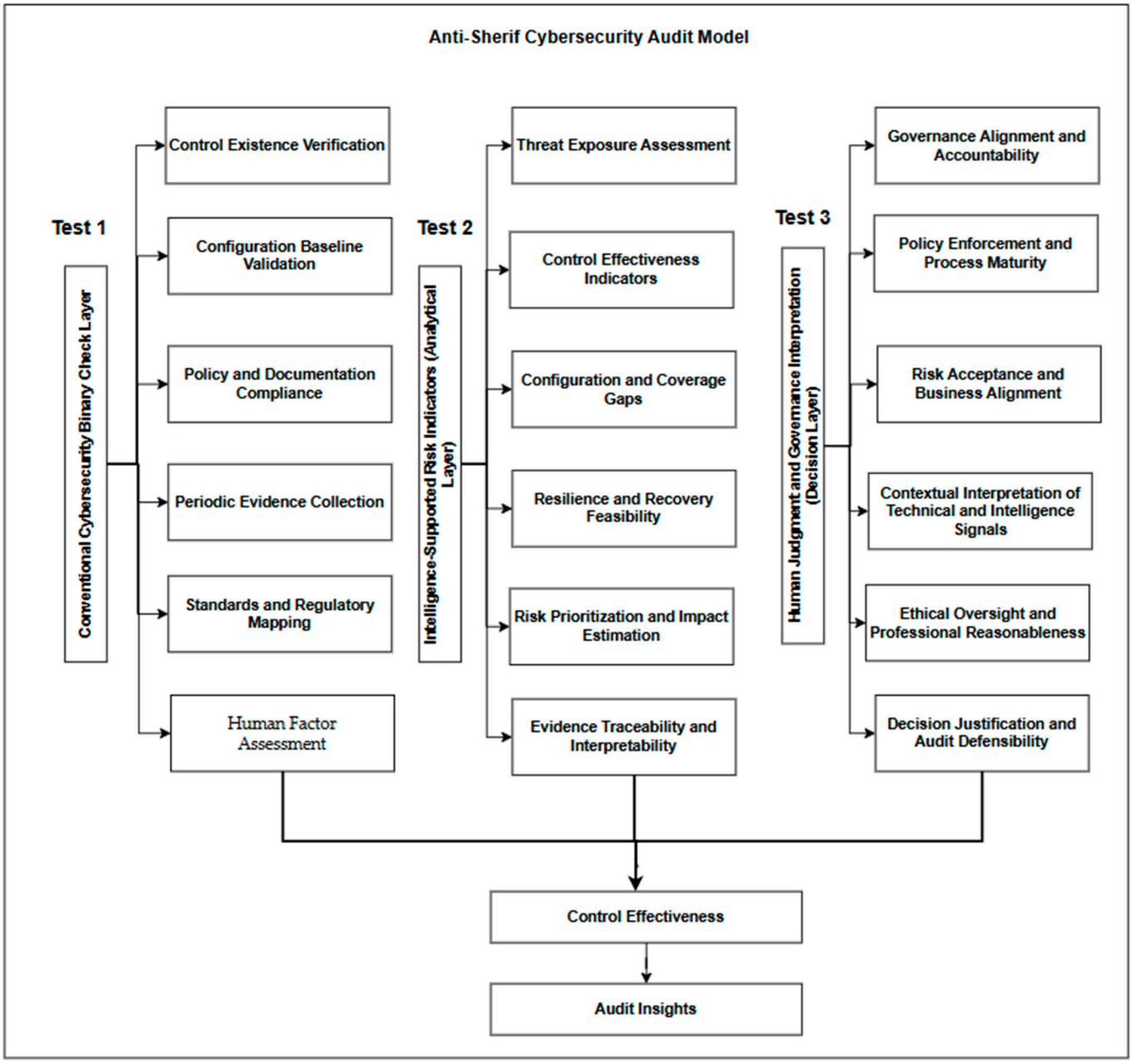

Figure 2. Conceptual high-level representation of the Anti-Sheriff Cybersecurity Audit Model.

As depicted in Figure 2, the Anti-Sheriff Cybersecurity Audit Model is structured into three interconnected layers, each representing a distinct audit test (Test 1–Test 3). These layers progressively and systematically enhance audit depth, transitioning from baseline compliance assurance to contextual, governance-aligned decision-making. The model culminates in an integrated evaluation of control effectiveness and the generation of meaningful audit insights. The different layers are expanded next.

5.1.1. Conventional Cybersecurity Binary Check Layer (Test 1)

The primary objective of a cybersecurity audit assessment is to assess whether technical controls are designed to satisfy the core complementary cybersecurity components, commonly referred to as the "security triad" [29] or Confidentiality, Integrity, and Availability (CIA). Organizations implement the CIA components through a range of mechanisms that protect the ICT environment. Traditionally, a confirmation of the existence of the controls was deemed sufficient to conclude on the testing results [33].

Within the contemporary ICT landscape, characterized by increasingly complex and sophisticated cyber threats, organizations invest in advanced detection mechanisms, including AI-assisted intrusion detection systems (IDS), security information and event management (SIEM), user and entity behavior analytics (UEBA), and endpoint detection and response (EDR); these identify malicious activities in near real time [23]. In parallel, organizations strengthen preventive capabilities through mechanisms such as operating system and database security hardening, network segmentation, multi-factor authentication (MFA), and AI-assisted controls that predict and block malicious activities in real time. Organizations also deploy security orchestration, automation, and response (SOAR) solutions to automate responses in near real time [34]. Advances in disaster recovery and backup planning further strengthen recovery capabilities.

Collectively, these mechanisms protect digital assets and align with the NIST Cybersecurity Framework (CSF) functions—protect, detect, respond, and recover [35]. These functions, derived from the NIST CSF [15], serve as essential building blocks for better cybersecurity hygiene.

To ensure that cybersecurity controls remain effective in supporting the CIA of information, organizations must perform regular cybersecurity auditing. Conventional approaches test the existence of these controls using binary compliance checks. As shown in Figure 2, traditional cybersecurity auditing practices are binary-based pass–fail; however, there is no doubt that within the proposed model, this layer establishes the minimum assurance baseline required for regulatory compliance and standard conformance. Table 2 presents the standard procedures that are performed during the conventional cybersecurity auditing, referred to as the "binary exercise".

As depicted in Table 2, the primary objective of conducting binary cybersecurity confirmation does not portray the value of conducting cybersecurity auditing, but rather enforces that certain controls should be in place for compliance purposes. In the modern era of sophisticated cybersecurity threats, this approach cannot effectively address cybersecurity risk [6]; hence, the stakeholders, if they do not see the value of cybersecurity auditing, will be reluctant to support the initiatives, even from a financial point of view.

In order to enhance the testing procedures presented in Table 2, the Conventional Cybersecurity Binary Check Layer (Test 1) testing procedures, the model introduces a second layer of testing, which initiates the intelligence-supported risk indicators that will move beyond a mere confirmation of the existence of cybersecurity controls.

Table 2. Conventional Cybersecurity Binary Check Layer (Test 1) testing procedures.

Control ID	Control Description	Example
BC1	Control Existence Verification	Confirms whether required cybersecurity controls (for example, SIEM, EDR, MFA, backups) are deployed within the ICT environment.
BC2	Configuration Baseline Validation	Verifies that implemented controls adhere to predefined baselines, vendor recommendations, or benchmark configurations (for example, CIS Benchmarks).
BC3	Policy and Documentation Compliance	Assesses the presence of formally approved policies, standards, and procedures governing cybersecurity controls.
BC4	Periodic Evidence Collection	Relies on point-in-time evidence such as screenshots, logs, configuration exports, and reports to substantiate audit findings.
BC5	Standards and Regulatory Mapping	Maps controls to external frameworks and regulatory requirements, such as ISO/IEC 27001, NIST CSF, and sector-specific regulations.
BC6	Pass–Fail Scoring Mechanism	Produces binary outcomes (compliant/non-compliant), which simplify reporting but provide limited insight into operational risk.

5.1.2. Intelligence-Supported Risk Indicators (Analytical Layer—Test 2)

As depicted in Figure 2, the second layer of the proposed model extends baseline compliance assessment by incorporating intelligence-supported analytical evaluation. This layer moves beyond mere control to assess how effectively cybersecurity controls operate in practice and how exposed they are to realistic and evolving cyber threats. Its primary objective is to contextualize compliance results within a threat-informed risk landscape, thereby addressing the limitations of traditional binary audit approaches.

As detailed in Table 3, the model is operationalized through a set of enhanced testing procedures designed to augment the binary checks performed in Test 1. For instance, Test Procedure 1 initially confirms the existence of a cybersecurity control, such as a Security Information and Event Management (SIEM) solution. While this satisfies baseline compliance requirements, it provides limited insight into the control's real-world effectiveness. In the second part of the proposed model, the assessment is extended by leveraging intelligence derived from the SIEM solution, particularly vulnerability and threat data, to evaluate exposure and exploitability. This intelligence-supported analysis enables a deeper understanding of the organization's cybersecurity posture by revealing how identified vulnerabilities intersect with active threat landscapes. Consequently, the organization gains a more accurate and actionable view of its cybersecurity state, supporting an informed risk-based decision-making process.

The necessity of human-in-the-loop principles within modern advanced technologies, including AI, has been widely emphasized in the literature. Researchers consistently argue that intelligent systems must be designed to support explainability, transparency, and accountability, particularly in high-stakes domains such as auditing and governance [36,37]. Within the cybersecurity auditing landscape, these attributes are critical to ensuring that analytical output remains interpretable, defensible, and aligned with professional judgment rather than operating as opaque decision mechanisms. In response to these concerns, the proposed Anti-Sheriff Cybersecurity Audit Model was expanded to explicitly incorporate human judgment and governance interpretation as a dedicated decision layer. This extension ensures that intelligence-supported indicators inform, rather than

replace, auditor reasoning, thereby preserving professional accountability while enhancing audit depth and relevance as presented next.

Table 3. Intelligence-Supported Risk Indicators (Analytical Layer—Test 2) testing procedures.

Control ID	Control Description	Example
RI1	Threat Exposure Assessment	Evaluates exposure to known and emerging threats using contextual indicators such as vulnerability, exploitability, and adversarial activity relevance.
RI2	Control Effectiveness Indicators	Examines operational performance metrics, including detection coverage, alert fidelity, response latency, and enforcement consistency.
RI3	Configuration and Coverage Gaps	Identifies partial deployments, misconfigurations, and blind spots that binary audits often overlook.
RI4	Resilience and Recovery Feasibility	Assesses the organization's ability to withstand and recover from cyber incidents, considering Return Time Objectives (RTOs), Return Point Objectives (RPOs), backup integrity, and recovery testing.
RI5	Risk Prioritization and Impact Estimation	Differentiates between low-impact compliance deviations and high-risk weaknesses that could materially affect business operations.
RI6	Evidence Traceability and Interpretability	Ensures that analytical indicators are transparent, explainable, and traceable to verifiable data sources, preserving audit defensibility.

5.1.3. Human Judgment and Governance Interpretation (Decision Layer—Test 3)

The invention of modern technologies, such as AI, has traditionally been associated with automation, hence the reduction in human intervention in pursuit of efficiency and accuracy. In certain domains, particularly auditing, including cybersecurity auditing, this assumption, however, presents a paradox [38]. While intelligence-driven automation enhances data processing, detection capabilities, and analytical depth, it does not eliminate the need for human involvement. On the contrary, cybersecurity auditing increasingly requires more deliberate and informed human engagement to interpret, contextualize, and govern the insights generated by automated intelligence capabilities. The outputs produced by systems—such as risk scores, anomaly detections, and predictive indicators—are not inherently meaningful without professional judgment to assess their relevance, ethical implications, and organizational context. As a result, rather than replacing auditors, the intelligence is meant to reshape their role, shifting it toward higher-order reasoning, critical evaluation, and accountable decision-making. In the proposed model, the author demonstrates the necessity of human-in-the-loop through some of the feasible testing procedures as depicted in Table 4.

As shown in Table 4, the human judgment and governance interpretation layer operationalizes professional oversight within the Anti-Sheriff Cybersecurity Audit Model by translating analytical findings into accountable and defensible audit conclusions. This layer evaluates governance alignment and accountability to ensure clear control, ownership, and escalation mechanisms, while assessing the maturity and consistency of policy enforcement using a structured, maturity-based approach. It further examines how residual risks are interpreted and managed in accordance with organizational risk appetite and business objectives. Intelligence-supported and technical signals are contextualized within the organization's operational, regulatory, and strategic environment to avoid misinterpretation. Ethical oversight and professional reasonableness are explicitly incorporated to prevent

over-reliance on automation and to ensure proportional, unbiased decision-making. Finally, all audit conclusions and recommendations are required to be clearly justified, documented, and explainable to stakeholders and regulators, thereby strengthening audit defensibility and trust.

Table 4. Decision Layer—Test 3—testing procedures.

Control ID	Control Description	Example
HJ1	Governance Alignment and Accountability	Evaluates clarity of control, ownership, escalation mechanisms, and accountability structures.
HJ2	Policy Enforcement and Process Maturity	Assesses how consistently cybersecurity processes are implemented, using a maturity-based evaluation (for example, CMM).
HJ3	Risk Acceptance and Business Alignment	Determines whether residual risks are consciously accepted, mitigated, or transferred in line with the organization's risk appetite and acceptability.
HJ4	Contextual Interpretation of Technical and Intelligence Signals	Interprets analytical findings within the organization's operational, regulatory, and strategic context.
HJ5	Ethical Oversight and Professional Reasonableness	Ensures audit decisions are proportionate, unbiased, and ethically defensible, avoiding over-reliance on automation.
HJ6	Decision Justification and Audit Defensibility	Requires that conclusions and recommendations are clearly justified, documented, and explainable to stakeholders and regulators.

The preceding discussions have provided a high-level representation of the proposed model. The subsequent section provides a detailed representation of the model and expands on its underlying logic, which follows the sequence binary check → Intelligence-Supported Risk Indicators → Human Judgment and Governance Interpretation.

5.2. Detailed Model Representation

As explained by Kaur et al. [39], modern cybersecurity applications aim to strengthen technical capabilities, including IDSs and intrusion prevention systems (IPSs). The concept of defense-in-depth plays a critical role in mitigating risks presented by complex cyber threats, such as APTs, ransomware, and zero-day exploits [40]. Technical cybersecurity controls remain essential, although a layered defense strategy is increasingly necessary to ensure resilience against sophisticated attacks in the modern threat landscape. Similarly, a layered cybersecurity auditing approach is essential, as demonstrated next.

5.2.1. A Detailed Model Components Description

In the present study, the proposed model uses multiple binary control checks and combines them into a unified set, as indicated in Equation (1). To ensure that the logic underlying the proposed model is scientifically and systematically sound, a set of mathematical assumptions and corresponding boundary conditions is defined. These assumptions provide a formal basis for structuring the model and for ensuring consistency across its analytical layers. The binary compliance testing exercise is conducted according to the logic and assumptions outlined below. All attributes, variables, and decision rules applied in this stage are direct extensions of the core conceptual model presented in Figure 2. The binary testing mechanism serves as the foundational layer of the model, upon which intelligence-supported analysis and human judgment are subsequently integrated, as demonstrated systematically next.

Let:

$$B = \{b_1, b_2, \ldots, b_6\};\ b_i \in \{0,1\}$$

where each binary component corresponds directly to the testing procedures presented in Table 1:

b_n: represent the binary check procedures.

The cumulative baseline checklist compliance score is defined as:

$$B_{avg} = \frac{1}{n}\sum_{i=1}^{n} b_i \in \{0,\ 1\} \quad (1)$$

Similarly, to Equation (1), the logic behind the intelligence threat exposure assessment is presented as follows:

Let:

$$I = \{i_1, i_2, \ldots, i_n\}\ i_j \in [0,\ 1]$$

where

i_n: represent threat exposure assessment procedures in Table 2; $i_j \in [0,\ 1]$

The analytical and intelligent risk score or indicator is defined as the cumulative of the following:

$$I_{avg} = \frac{1}{n}\sum_{j=1}^{n} i_j\ ;\ \ i_j \in [0,\ 1] \quad (2)$$

The last part of the proposed model is the integration of human judgment into the model. This is mathematically presented as follows:

Let:

$$H = \{h_1, h_2, \ldots, h_k\}$$

where

h_k: represents governance alignment and accountability testing procedures defined in Table 3; and $h_k \in \{0,\ 1\}$

The governance judgment score is:

$$H_{avg} = \frac{1}{n}\sum_{k=1}^{n} h_k\ \ h_k \in \{0,\ 1\} \quad (3)$$

As alluded to by Zahed et al. [13], most cybersecurity frameworks and standards are diagnostic, not quantitative. They help organizations name, classify, and prioritize threats, but they stop short of answering the harder question: "How much risk do we actually have?" In a quest to quantify human judgment in the auditing of cybersecurity controls, the authors apply the Capability Maturity Model (CMM) and assign scores based on expert assessment. The base score applied in this study ranges from 0 to 1, ensuring alignment with the binary checklist defined earlier. The reason for employing the CMM is to align with the variable defined within the binary check and the intelligent risk indicators. In addition, the CMM was deemed appropriate for benchmarking human judgment using a well-established and widely recognized metric. Importantly, as depicted in Table 5, the assigned base scores are neither intrusive nor computed by the authors; rather, they are values defined by the CMM reference model itself.

Table 5. Cybersecurity control evaluation reference according to the CMM framework.

CMM Level	Description [41]	Interpretation in the Cybersecurity Audit Context	Assigned Base Score (H_i)
Level 1 Initial (Ad hoc)	At this level, organizational processes are chaotic and disorganized, and the initiatives are conducted haphazardly.	Cybersecurity governance is largely reactive; accountability is unclear, decisions are undocumented, and reliance on informal judgment dominates.	0.2
Level 2 Repeatable/managed	Basic processes are established, however, at an entry level.	Governance roles and policies exist, but enforcement is irregular; risk decisions are made, but not systematically aligned to business objectives.	0.4
Level 3 Defined	At this level, the process is standardized, documented, and integrated throughout the organizational structure.	Governance structures are defined; policy enforcement is consistent; audit decisions are documented and contextually justified.	0.6
Level 4 Quantitatively managed	Metrics are key performance indicators (KPIs) defined against the processes for qualitative and quantitative measurements of success factors.	Governance effectiveness, policy enforcement, and risk acceptance decisions are supported by measurable indicators and repeatable evaluation criteria.	0.8
Level 5 Optimizing	Processes are grounded, and the organization focuses on continuous improvements.	Human judgment is formally integrated with intelligence-supported insights; ethical oversight is explicit, decisions are defensible, and governance continuously evolves based on lessons learned.	1

Now that all variables entailed in the model have been mathematically denoted, the overall model outcome can be computed as the final Anti-Sheriff Control Effectiveness Score (CES). The CES represents a composite measure of cybersecurity control effectiveness and is defined as a weighted integration of the three core layers of the proposed model, namely: (i) binary compliance assessment, (ii) intelligence-supported risk analysis, and (iii) human judgment evaluation. Formally, the CES aggregates these layers through a weighted summation model that can be defined as follows:

$$CES = \alpha B_{avg} + \beta I_{avg} + \gamma H_{avg} \quad (4)$$

subject to:

$$\alpha + \beta + \gamma = 1 \quad (5)$$

where:

α emphasizes compliance assurance

β emphasizes risk exposure and resilience

γ emphasizes governance and professional judgment

The Audit Insight Output (AI^*) is a function of control effectiveness and organizational context:

$$AI^* = f\left(CES, R_{appetite}, B_{impact}\right) \quad (6)$$

where:

$R_{appetite}$ = organizational risk appetite

B_{impact} = business impact severity

Now that all the formulas adopted in the present study have been expanded in detail, it is also essential to present a proposition that proves that nesting (layered approach) of audit assurance layers guarantees better results as opposed to a binary check. This proposition is grounded in the mathematical approach of Matryoshka ("nested dolls") [42]. A Matryoshka-style model refers to "*a hierarchical and recursive structure in which each analytical layer encapsulates a complete but progressively refined representation of the system under assessment*" [42].

Let $B_{avg} \in [0,\ 1]$ denotes the average binary compliance score derived from conventional cybersecurity audit procedures, where controls are evaluated solely on existence or pass–fail criteria. Let $I_{avg} \in [0,\ 1]$ represent the intelligence-supported analytical risk indicators, and let $H_{avg} \in [0,\ 1]$ denotes the governance and human judgment score derived from maturity-based assessment. Then, achieving a high value of B_{avg} alone is a necessary but not sufficient condition for high cybersecurity control effectiveness outcome of the overall audit process.

Formally, the composite control effectiveness score can therefore be computed as follows:

$$CES = \alpha B_{avg} + \beta I_{avg} + \gamma H_{avg} \quad where \quad \alpha + \beta + \gamma = 1$$

This implies that $B_{avg} \approx 1 \not\Rightarrow CES \approx 1$, unless I_{avg} and H_{avg} are also sufficiently high. With this proposition, certain assumptions can now be made, and the proof of the proposed model can be done using counterexamples. In essence, these composites mean that even in cases where the binary check outcome is favorable, the final control effectiveness score is not inherently high, unless both the intelligent and human indicators are also high.

Expanding on this proposition, let us consider an auditee ICT environment for which most, if not all, required cybersecurity controls are formally implemented and documented. Under a conventional cybersecurity audit approach, the results can be denoted as:

$$B_{avg} = 1$$

Under the following condition:

Analytical weakness:

The implemented controls are misconfigured, poorly tuned, or exposed to high-likelihood threats (for example, unpatched vulnerabilities, ineffective alerting, and unrealistic recovery objectives). Consequently, $I_{avg} \ll 1$.

Governance weakness:

Similarly, if the control ownership is unclear, risk acceptance decisions are either undocumented, recovery plans are untested, or audit conclusions cannot be defensibly justified to regulators the, $H_{avg} \ll 1$.

Substituting the composite score, the final composite control effectiveness can be denoted as $CES = \alpha B_{avg} + \beta I_{avg} + \gamma H_{avg}$ this is because $\beta, \gamma > 0$ by construction of the Anti-Sheriff model, the low values of I_{avg} and H_{avg} dominate the final score, which yields a yield of $CES < 1$.

As observed from the demonstration, the defined proposition proof on its own indicates that, despite perfect binary compliance, the overall cybersecurity control effectiveness can remain low if other factors, such as risk intelligence indicators and human judgment, are taken into consideration. This contradicts the implicit assumption of traditional audits that high compliance equates to low risk, thereby proving that binary checks alone can be misleading. As also emphasized by Mohawesh et al. [6]. Considering conditions and different scenarios during the cybersecurity auditing process is a progressive step towards a shift from a mere binary check exercise to a more risk-based approach.

Just like any other traditional financial audit, cybersecurity audits are inherently time-bound activities, meaning that at a defined point, the audit must conclude and its outcomes must be formally communicated to relevant stakeholders. Within this constraint, achieving reasonable audit coverage remains essential to ensure that material risks associated with the auditee are adequately identified and assessed. To address this requirement, the next section introduces a guided approach for grouping related testing procedures across the three layers. This grouping mechanism supports efficient audit execution while preserving

the model's objective of moving beyond checklist-based compliance toward risk-informed and defensible cybersecurity audit outcomes.

5.2.2. Cybersecurity Procedures Grouping

Table 6 summarizes how the Anti-Sheriff Cybersecurity Audit Model groups binary checks, intelligence-supported risk indicators, and human judgment procedures, which can be organized into coherent audit objectives that must be executed together to achieve meaningful assurance. Rather than treating compliance, technical analysis, and governance as independent activities, the proposed model aligns these procedures to address specific assurance goals, such as validating control configuration, distinguishing compliance from effectiveness, assessing threat-driven risk, evaluating operational resilience, supporting risk-based decision-making, and ensuring audit defensibility. As denoted in the table testing procedure, for example, BC1, BC2, RI3, and HJ4 can be executed together for a sound cybersecurity audit outcome. These groups are essential to address different cyber risks distribution, such as cloud risk, general risk, and internal deficiency [43].

Table 6. Anti-Sheriff Cybersecurity model procedure grouping.

Audit Objective (Group)	BC	RI	HJ
Control Validity & Configuration Assurance	BC1, BC2	RI3	HJ4
Compliance vs. Effectiveness Distinction	BC3	RI2	HJ2
Threat-Driven Risk Assessment	BC1, BC2	RI1	HJ4
Operational Resilience & Recoverability	BC4	RI4	HJ1
Risk Prioritization & Decision Support	BC6	RI5	HJ3
Audit Defensibility & Regulatory Trust	BC3, BC5	RI2, RI5	HJ6, HJ5

Now that the procedures have been grouped accordingly, before applying the model using a case scenario, it is vital to summarize the flow process of the proposed model. The Anti-Sheriff Cybersecurity Audit Model is grounded in the principle that assurance should enable risk understanding and improvement rather than enforce compliance through punitive, checkbox-driven assessments. Figure 3 is a demonstration of the logic process of the proposed model. The finer details of the figure are presented after the graphic representation.

As depicted in Figure 3, Test 1 (the binary test procedure) serves as a foundational entry point where conventional cybersecurity binary checks are performed to verify the existence of cybersecurity controls, configuration baselines, and policy compliance. Importantly, in the proposed model, this stage is not treated as an enforcement mechanism; therefore, passing this phase does not terminate the audit but instead initiates baseline control remediation, reinforcing the Anti-Sheriff philosophy that audits should support control maturity and organizational learning rather than induce fear or concealment.

Once the baseline is established, the audit advances to Test 2, where the Anti-Sheriff approach becomes more pronounced through the use of intelligence-supported risk analysis. At this stage, technical compliance results are augmented with intelligent risk indicators such as threat exposure, exploitability likelihood, and external exploit signals. This ensures that controls are not merely present but are assessed for their real-world effectiveness against evolving threat conditions. Rather than issuing blanket findings, the model distinguishes between acceptable and elevated risk, enabling risk-informed control hardening where necessary and avoiding unnecessary remediation where controls are sufficient.

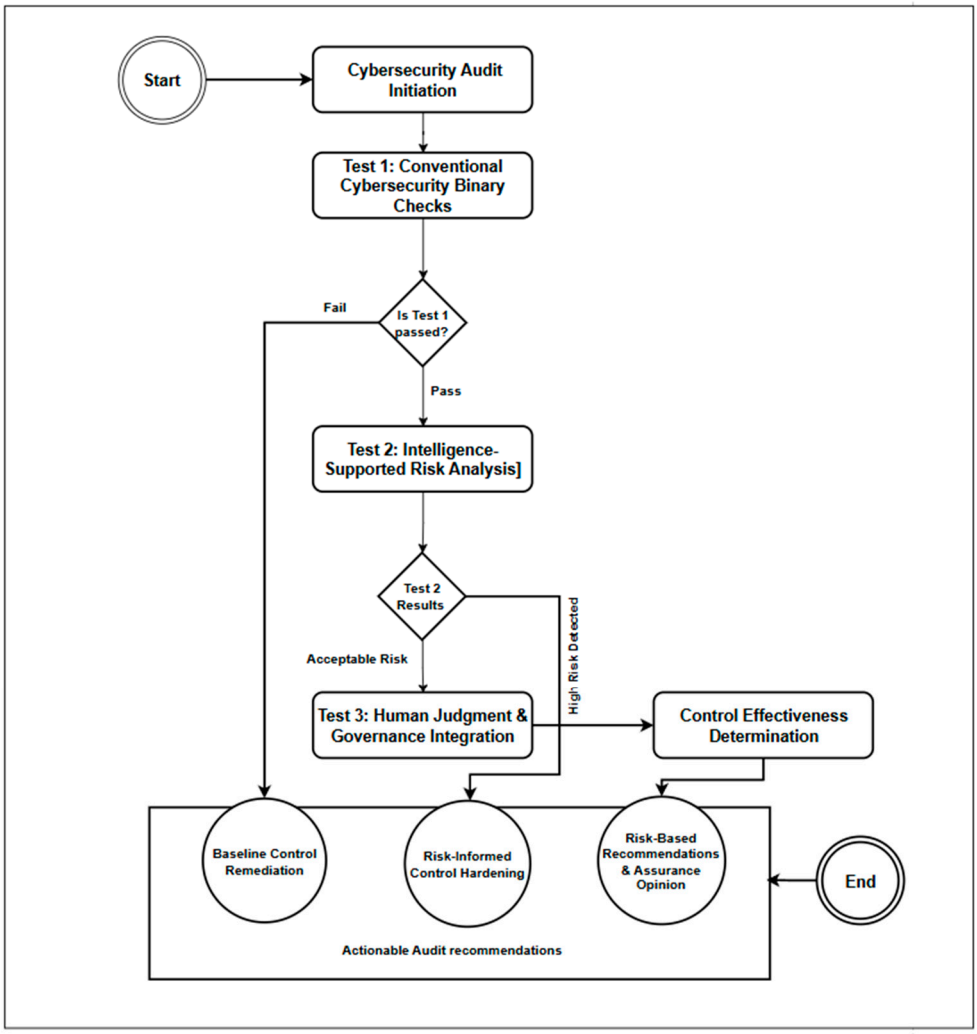

Figure 3. Anti-Sheriff Cybersecurity Audit Model flow diagram.

Finally, Test 3 embodies the final aspects of the Anti-Sheriff Cybersecurity Audit Model by integrating human judgment, governance considerations, and ethical reasoning into the audit outcome. This stage ensures that audit conclusions are not automated or mechanistic, but instead reflect professional reasoning aligned with governance structures and business objectives.

At this point, the authors have presented the model in a compendium. As demonstrated by Rananga and Venter [2], and by Sánchez-Paniagua et al. [44], experimental demonstrations play a critical role in establishing the applicability of a proposed solution through the use of fictional scenarios that closely reflect real-world conditions. The cruciality of empirical demonstrations through case scenarios was also emphasized by Al-Matari et al. [28]. The subsequent subsection applies the proposed model to such a case study and provides an empirical analysis. This is done to practically demonstrate how the proposed model can enhance the cybersecurity audit from a mere tick-box exercise to a more intelligence-based approach.

5.3. Empirical Research

To support clarity in the empirical demonstration of the proposed model, the study presents a fictional logical case scenario. In practice, such a scenario would correspond to a business case or an audit requirement defined within the audit scope, depending on the organization's risk appetite.

5.3.1. Fictional Case Scenario

Nany FinTrust MicroBank (Pty) Ltd. is a fictional SME specializing in micro-lending services. The institution employs approximately 200 staff members and operates under a hybrid working arrangement supporting remote and office-based work. Due to the nature of its services, the institution subscribes to several regulatory and data privacy standards, including the Protection of Personal Information Act (POPIA), the Payment Card Industry Data Security Standard (PCI DSS), the NIST CSF, and the CIS Benchmarks. These standards represent commonly adopted cybersecurity and data protection frameworks, as expressed by Sulistyowati et al. [11].

In recent audit cycles, the organization's cybersecurity posture was assessed as largely satisfactory based on conventional cybersecurity audit practices. The most recent audit report concluded that the majority of required security controls were implemented and compliant with applicable standards, resulting in a favorable audit outcome. Consequently, management and key stakeholders were led to believe that the institution's cybersecurity controls were adequate and that residual risk was acceptably low.

Shortly thereafter, however, Nany FinTrust MicroBank experienced a cybersecurity incident involving unauthorized access to sensitive customer data processed by remote endpoints. The incident resulted in operational disruption and recovery costs amounting to several thousand rand, involving forensic investigations, system remediation, and regulatory response activities. The occurrence of this breach directly contradicted the earlier audit assurance and raised serious concerns regarding the reliability and depth of the existing cybersecurity audit approach.

In response, senior management questioned how a material cybersecurity incident could occur in an environment that had recently been assessed as compliant and secure. This prompted a request for a root-cause analysis to determine whether the breach resulted from control failure, misconfiguration, governance weaknesses, or limitations inherent in the audit methodology itself.

In the next section, our model is applied to evaluate selected cybersecurity controls, focusing on uncovering the underlying causes of the incident and providing management with actionable, defensible insights into residual risk, control effectiveness, and governance maturity.

5.3.2. Experimental Demonstration

Before delving deep into the demonstration of the model in the scenario, the study defines the variables used throughout the experiment through variable operationalization. Variable operationalization translates abstract research concepts into measurable indicators supporting empirical and quantitative observation [11], as summarized in Table 7.

Table 7. Experimental variable operationalization.

Construct	Symbol	Measurement Approach	Data Type
Compliance check	B_{avg}	Binary assessment of control implementation: 0 = not implemented, 1 = implemented	Binary (Discrete)
Intelligence-supported risk indicators	I_{avg}	ML-derived exploit likelihood/risk probability, normalized to the range [0, 1]	Continuous
Human Judgment Integration (Using CMM levels)	H_{avg}	Derived from Table 3 maturity scale (0.2–1.0)	Ordinal → Continuous (mapped)
Controlled weights	α, β & γ	$\alpha + \beta + \gamma = 1$	Continuous (fixed parameters)
Control Effectiveness Score (CES)	CES	$\alpha B_{avg} + \beta I_{avg} + \gamma H_{avg}$	Continuous

In practical applications, the weights presented in Table 7 can be computed using methods, such as a Delphi-based expert process, informed by historical cybersecurity incident data. For this demonstration, the study defines the weights using proportional influence. The weighting parameters remain bounded within the interval $[0 : 1]$ to regulate the relative contribution of each scoring dimension. The cybersecurity audit focus was narrowed to reflect the defined case scenario. The auditor established the technical boundaries and identified the in-scope systems for evaluation. As already mentioned, audit exercises are inherently scope-defined, meaning that an audit cannot assess all controls simultaneously. To ensure meaningful outcomes, auditors commonly adopt risk-based approaches [3]. For the sake of this demonstration, and guided by control grouping in Table 4, the Nany FinTrust MicroBank scenario was explicitly tested using BC1, BC2, RI3, and HJ4 testing procedures. For ease of reference, a part of the model flow diagram that is being demonstrated is highlighted as presented in Figure 4.

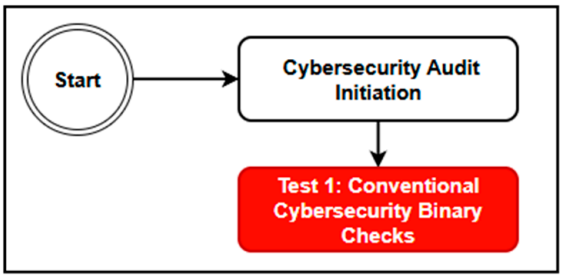

Figure 4. Anti-Sheriff cybersecurity audit test being demonstrated (Binary layer (Compliance check)).

Step 1: Binary layer (Binary check exercise). In this step, the audito test the controls in scope guided by the defined group, and the results are recorded accordingly.

We apply two binary procedures:

BC1 (Control Existence Verification): EDR is deployed $\rightarrow b_1 = 1$

BC2 (Configuration Baseline Validation): Baseline exists (documented standard build) $\rightarrow b_2 = 1$

Binary average: $B_{avg} = \frac{b_1 + b_2}{2} = \frac{1+1}{2} = 1.0$

Conventional audit interpretation: "Control is compliant/present."

At this stage, the results of the conventional cybersecurity audit indicate the existence of both BC1 and BC2. As illustrated earlier in the model flow diagram (Figure 3, the confirmation of these baseline controls satisfies the binary compliance requirements and consequently triggers the subsequent phase of the proposed model.

Step 2: Intelligence-supported layer (RI1: Threat Exposure Assessment)

In this step as demonstrated in Figure 5, a network tool is run targeting the ICT environment of Nany FinTrust MicroBank (Pty) Ltd. to identify common vulnerabilities and exposures (CVEs) affecting the server infrastructure, and the model assesses the likelihood of exploiting these CVEs with limited effort using the exploit prediction scoring system (EPSS) [12]. EPSS derives its score from the output of the network scanning tool used in the experimental demonstration. Similar to the CMM values, the EPSS values were sourced from established exploit-probability metrics and were not generated by the authors. For clarity, this tool is referred to hereafter as "the Network Tool". From the Network Tool's scan results, it can be assumed that 15 CVEs were found from identified critical vulnerabilities, as recorded in Figure 6.

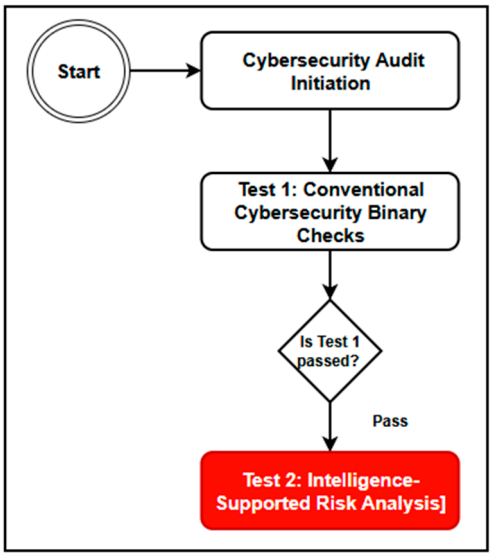

Figure 5. Anti-Sheriff Cybersecurity audit test being demonstrated (Intelligence-supported layer).

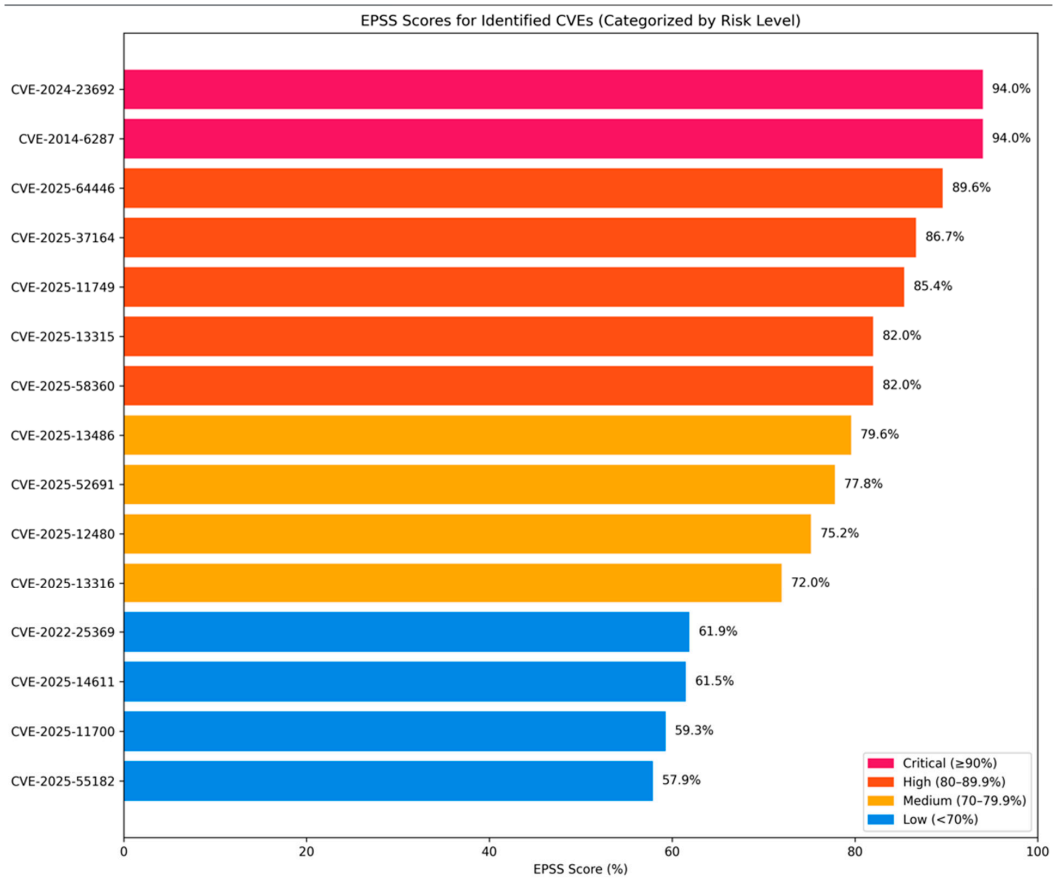

Figure 6. Base exploit prediction scoring system (EPSS) scores obtained from the National Vulnerability Database (NVD) [45].

As shown in Figure 6, the EPSS values associated with the identified CVEs indicate the likelihood of exploitation of the identified CVEs from 57.9% up to 94.0%. While this result provides a robust initial indication of risk, the proposed model applies additional mechanisms to substantiate the probability rationale and derive an intelligence risk indicator.

At this point, the model introduces an algorithm incorporating open-source intelligence (OSINT). Public repositories frequently provide guidance and proof-of-concept (PoC)

material for exploiting, known as CVEs. In the present study, GitHub serves as the primary OSINT source because of its widespread adoption, accessibility, and support for application programming interface (API) integration, which are required for the search algorithms presented in Algorithm 1 (accessed on 12 February 2026). Prior studies, including Cosentino et al. [46] and Wang et al. [46], also identify GitHub as a dominant platform for publicly shared vulnerability-related artifacts.

As illustrated in Algorithm 1, the algorithm automates the assessment of online visibility and exploitation maturity for a provided CVE by querying GitHub for publicly accessible references linked to that vulnerability. The process constructs a search query using the CVE identifier and submits it to the GitHub Search API. The API returns repositories, commits, issues, and code fragments containing the CVE identifier. The algorithm then extracts the total number of references and applies a predefined bucket-based normalization scheme to transform the raw count into a standardized score within the interval $[0, 1]$. Lower reference counts correspond to lower scores, indicating limited public exploitation activity, whereas higher counts map to values approaching 1.0, indicating either extensive discussion, available PoC material, or operational weaponization. The resulting normalized OSINT-derived metric feeds into the broader intelligence scoring computation used to evaluate cybersecurity controls within the proposed model.

Algorithm 1 Computer INTELLIGENCE From GitHub CVEs Mentions $AM \in [0, 1]$

1: **Procedure** Normalized Mention Score M
2: **Input:** $(\boldsymbol{CVE\_ID})$
3: **Output: Normalized Mention Score** M
4: **Step 1:** Build Search Query for the CVEs found during Network Scan Results
5 : $query \leftarrow$ " *https://api.github.com/search/code?q=* " $+ \ CV\ E\ ID$
6: **Step 2:** Send REST API Request and get response with total mentions about the CVEs found from the Network Scan results
7 : $response \leftarrow HT\ T\ P.GET\ (query)$
8: **Step 3:** Apply Normalization (Predefined Logic)
9: **if** $total\_mentions = 0$ **then**
10 : $M \leftarrow 0.0$
11: **else if** $1 \leq total\_mentions < 5$ **then**
12 : $M \leftarrow 0.2$
13: **else if** $5 \leq total\_mentions < 20$ **then**
14 : $M \leftarrow 0.4$
15: **else if** $20 \leq total\_mentions < 50$ **then**
16 : $M \leftarrow 0.6$
17: **else if** $50 \leq total\_mentions < 100$ **then**
18 : $M \leftarrow 0.8$
19: **else**
20 : $M \leftarrow 1.0 \triangleright$ Highly discussed widely weaponised
21: **end if**
22: **Step 4: Return Normalized Score**
23: **return** M
24: **end procedure**

Expanding from the presented algorithm as depicted in Algorithm 1, a Python 3 script is used to validate the applicability of the proposed algorithm by retrieving results through the GitHub search functionality. For demonstration purposes, the script uses the

identified CVEs as input and records the corresponding outputs, as illustrated in Figure 7 and summarized in Table 8.

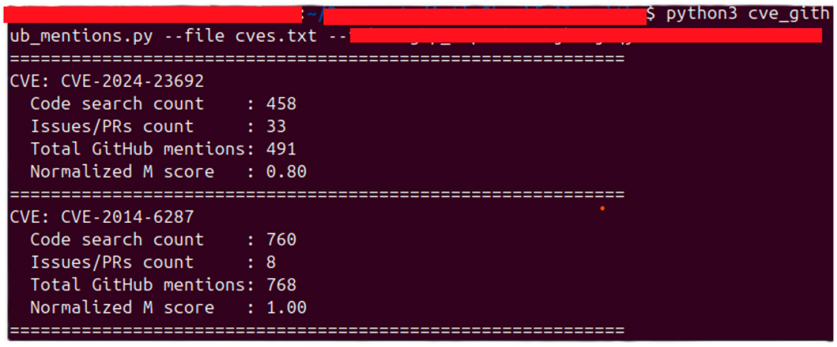

Figure 7. Script results.

Table 8. GitHub-Derived Exploitability Intelligence for identified CVEs.

ID	CVE ID	Code Search Count	Issues/PRs Count	Total GitHub Mentions	Normalized M Score
1	CVE-2024-23692	458	33	491	0.80
2	CVE-2014-6287	760	8	768	1.00
3	CVE-2025-64446	370	57	427	0.80
4	CVE-2025-37164	330	45	375	0.80
5	CVE-2025-11749	160	12	172	0.60
6	CVE-2025-13315	87	8	95	0.60
7	CVE-2025-58360	190	47	237	0.80
8	CVE-2025-13486	84	14	98	0.60
9	CVE-2025-52691	344	26	370	0.80
10	CVE-2025-12480	224	15	239	0.80
11	CVE-2025-13316	70	3	73	0.60
12	CVE-2025-25369	11	0	11	0.40
13	CVE-2025-14611	79	11	90	0.60
14	CVE-2025-11700	62	13	75	0.60
15	CVE-2025-55182	820	105,777	106,597	1.00

As indicated in Figure 7, the methodology used in the proposed model to compute the final normalized value incorporates three GitHub-derived intelligence signals: code search counts, issues and pull requests (PRs), and the total number of references to a vulnerability across GitHub repositories. The algorithm aggregates these signals and applies the normalization thresholds defined earlier in Algorithm 1 to derive the threat intelligence score M.

The vulnerability CVE-2024-23692, identified during, for example, the ICT vulnerability scan of the fictional organization Nany FinTrust MicroBank (Pty) Ltd., was processed using the Python script. The results, presented in Table 8, indicate 458 code references and 33 issue or PR references, yielding a combined total of 458 GitHub references associated with this CVE. Applying the normalization rules defined in Algorithm 1, the final normalized score for CVE-2024-23692 is 0.80, reflecting a high level of community attention, exploit maturity, and threat relevance. The same computational logic applies consistently to all CVEs included in the demonstration, and the results are recorded in Table 8 accordingly.

In the proposed model, the Normalized M Score is used as a direct indicator of exposure, capturing how visible and actionable a vulnerability is in the public domain.

Exposure, in this context, refers not merely to the existence of a weakness, but to the degree to which that weakness is accessible, reproducible, and actively leveraged by attackers or security practitioners. By aggregating GitHub code references, issues, and pull requests, the M score reflects the practical ease with which an exploit can be discovered, adapted, and deployed.

A high M score (e.g., M = 1.00), for example, as observed for CVE-2014-6287 and CVE-2025-55182, signals maximum exposure. These vulnerabilities exhibit extensive exploit artifacts and sustained community interaction, meaning that attackers face minimal effort in weaponizing them. In Anti-Sheriff terms, this represents a scenario where exposure is already realized, not theoretical. Even if baseline controls (BC) exist, such exposure significantly elevates residual risk, making these CVEs critical drivers in the Risk Intelligence (RI) layer and, ultimately, in the CES computation.

Moderate M scores (M $\approx$ 0.80)—such as those for CVE-2024-23692 and CVE-2025-52691—indicate active and growing exposure. These vulnerabilities are well-documented and supported by usable exploit references, but have not yet reached full saturation. In the model logic, this represents a dangerous transition state: exposure is sufficiently high to warrant concern, yet often underestimated in conventional audits that stop at control existence. The Anti-Sheriff approach deliberately elevates such cases to prevent delayed responses.

At this point, as demonstrated by the intelligence risk indicator, the high-risk results have already emerged from Step 2; hence, further scrutiny using the subsequent analytical step is not required for risk confirmation, as illustrated in the model flow diagram (Figure 3). The intelligence-supported assessment has provided sufficient evidence to substantiate elevated exposure and exploitability, thereby satisfying the model's criteria for risk escalation and prioritization.

Consequently, the demonstration of the proposed model proceeds directly to the final audit stage, namely the insight layer, as depicted in Figure 8. This stage does not seek to revalidate risk, but rather to translate the identified high-risk conditions into actionable insights, decision support, and governance-relevant conclusions. In doing so, the model reinforces its Anti-Sheriff philosophy by emphasizing informed judgment and practical outcomes over redundant control re-examination.

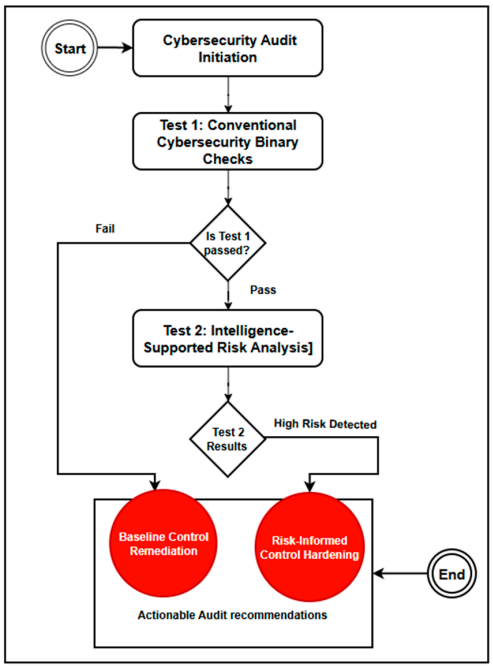

Figure 8. Anti-Sheriff Cybersecurity audit test being demonstrated (Actionable Audit Recommendation).

Based on the intelligence gathered from OSINT sources and EPSS metrics, the auditor can reasonably infer the following root causes of the recent cybersecurity incident experienced by Nany FinTrust MicroBank (Pty):

- The scope of the recent cybersecurity audit was not risk-based, which may have resulted in a misleading assurance outcome. The audit primarily emphasized control existence rather than evaluating exposure, exploitability, and threat relevance, thereby underestimating material cyber risk.
- The audit approach adopted was largely a tick-box exercise, aimed at confirming the presence of cybersecurity controls, without adequately incorporating public-domain intelligence, exploiting maturity, or paying attention to active threat indicators. As a result, critical vulnerabilities with high exploit likelihood were not sufficiently prioritized.
- The cybersecurity audit placed limited emphasis on business continuity considerations, particularly key operational parameters such as the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). This disconnect between technical control assessment and business impact weakened organizational preparedness and resilience.

To further elaborate on the demonstration, Figure 9 extends the intelligence-gathering capabilities of the proposed model by establishing a direct relational mapping between EPSS scores and the normalized OSINT exploitability value (M score). This alignment enabled a comparative analysis between predicted exploit likelihood and observed exploit maturity and prevalence, thereby revealing convergence and divergence patterns between the two dimensions. By integrating these complementary signals, the model moves beyond binary compliance and single-metric prioritisation, supporting a more nuanced, intelligence-driven assessment of cybersecurity risk consistent with the Anti-Sheriff auditing cybersecurity approach.

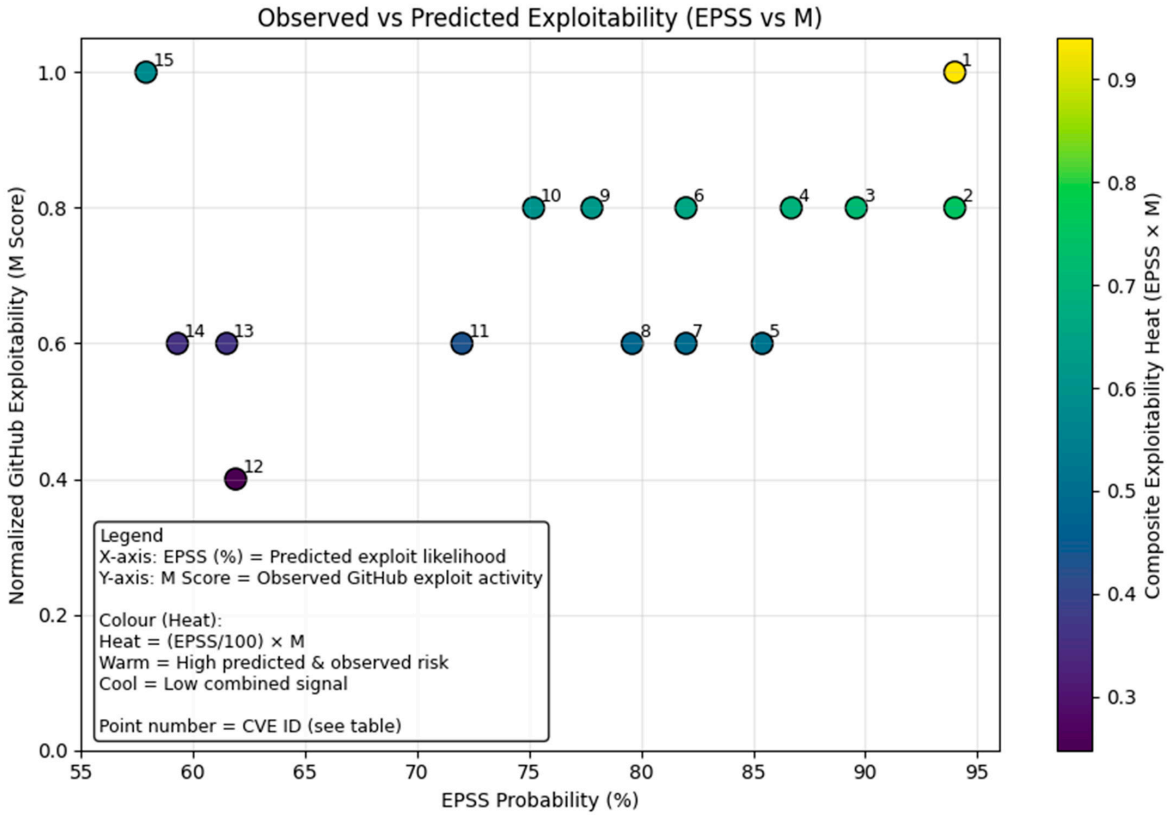

Figure 9. Enhanced intelligence using EPSS and the OSINT.

As depicted in Figure 9, the x-axis represents *EPSS* percentage, indicating the predicted likelihood that a vulnerability will be exploited in the wild. The y-axis represents the Normalized GitHub Exploitability Score ($\boldsymbol{M}$), capturing observed public exploit activity based on code repositories, issues, and pull requests. Each plotted point corresponds to a CVE and is labeled using a numeric identifier, which maps to the full CVE details in the accompanying Table.

The color intensity of each point reflects a composite exploitability heat value, calculated as:

$$Heat = \frac{EPSS}{100} \times M$$

Warmer colors (yellow–green) indicate vulnerabilities with both high predicted exploitation likelihood and high observed exploit activity, representing confirmed operational risk. Cooler colors (blue–purple) indicate lower combined exploitability signals. This visualization highlights discrepancies between predictive risk models and real-world adversarial behavior, thereby supporting an intelligence-driven, Anti-Sheriff cybersecurity auditing approach.

The figure compares predicted exploit likelihood (*EPSS*) with observed exploit activity on GitHub (M score) for individual CVEs. A CVE, for example, plotted near 94–95% *EPSS* with an M score of 1.0 (top-right of the chart) indicates a vulnerability that is not only highly likely to be exploited according to predictive intelligence, but also shows strong real-world exploit activity. This alignment represents a high-confidence, high-risk case that warrants immediate attention. In contrast, some CVEs show high *EPSS* but only moderate observed activity, such as those around 85–90% *EPSS* with $M \approx 0.6$–0.8. These cases suggest vulnerabilities that are technically attractive to attackers and likely to be exploited, but where widespread public exploit code or discussion has not yet fully materialized. Such CVEs are important early-warning signals, where proactive mitigation can prevent future exploitation.

The chart also highlights mismatches between prediction and observation. For instance, CVEs around 60–62% EPSS display a wide range of M scores, from low ($\approx$0.4) to high ($\approx$1.0). This shows that some vulnerabilities with modest predicted likelihood may still experience significant exploit activity due to factors such as ease of exploitation, popularity of affected software, or attacker trends. These examples demonstrate why combining *EPSS* with observed exploit evidence, as done in the Anti-Sheriff model, provides a more accurate and defensible basis for cybersecurity risk prioritization, rather than relying on either metric alone. Moreover, as a root cause of the recent experienced cyber incident for the defined case scenario, it is not evident why it is essential to move beyond a mere cybersecurity control existence confirmation in this modern era of advanced, complex, and sophisticated cyber threats.

The study model demonstration concludes with a comparative analysis of a conventional binary check exercise and the hybrid control assessment, summarized in Table 9.

To further substantiate the rationale underpinning the proposed model, Table 9 illustrates the necessity of moving beyond cybersecurity auditing as a mere tick-box or binary compliance exercise. A practical example of the limitations inherent in binary checks can be observed in firewall rule management. Using the BC1 testing procedure, an auditor may successfully confirm the presence of required controls and verify that a firewall is implemented and operational. Such verification alone, however, is insufficient to identify critical weaknesses, including overly permissive any–any rules, unused legacy rules supporting decommissioned systems, or the absence of proper network segmentation between critical business systems and less-trusted network zones. In these scenarios, the control formally exists and therefore passes the audit, while simultaneously introducing significant exposure to lateral movement, privilege escalation, and data exfiltration risks that directly

threaten business operations. This misalignment between compliance status and actual security posture highlights a fundamental weakness of binary auditing approaches.

Table 9. Comparison of binary and hybrid control assessment.

Assessment Dimension	Binary Compliance Cybersecurity Audit Approach	Hybrid Anti-Sheriff Cybersecurity Audit Model (BC + RI + HJ Procedures)
Primary audit focus	Verification of control existence and formal compliance	Holistic evaluation of compliance, inherited risk, and governance maturity
Control existence verification	BC1: Confirms presence of required controls	BC1 retained, but existence is treated as a baseline prerequisite, not an outcome
Configuration assessment	BC2: Validates alignment with baselines and benchmarks	BC2 + RI3: Identifies misconfigurations, partial deployments, and blind spots
Policy and documentation review	BC3: Confirms existence of approved policies	BC3 + HJ1/HJ2: Evaluates governance clarity, enforcement consistency, and maturity
Evidence collection approach	BC4: Point-in-time, static evidence	BC4 + RI6 + HJ6: Continuous, explainable, and traceable evidence supporting defensible judgments
Standards and regulatory mapping	BC5: Maps controls to frameworks and regulations	BC5 + RI5 + HJ3: Distinguishes formal compliance from material business risk
Human factor consideration	BC6: Confirms training existence	BC6 + HJ2/HJ5: Assesses process maturity, ethical oversight, and professional reasonableness
Threat landscape sensitivity	None (implicit assumption of stable threats)	RI1: Explicit evaluation of current and emerging threat exposure
Control effectiveness evaluation	Implied through compliance status	RI2: Measured using operational performance indicators (coverage, fidelity, and response)
Resilience and recovery assessment	Typically out of scope	RI4: Evaluates RTOs, RPOs, backup integrity, and recovery feasibility
Risk differentiation	Low—all deviations treated similarly	RI5: Differentiates low-impact gaps vs. high-impact cyber risk
Contextual interpretation	Not performed	HJ4: Interprets technical and intelligence findings within organizational context
Decision rationale	Checklist-driven conclusions	HJ6: Explicitly justified, explainable, and auditable decisions
Overall outcome	Statement of compliance	Risk-informed judgment on control effectiveness and residual risk

The proposed model addresses this gap by integrating intelligence-supported risk indicators, including insights derived from OSINT. Sources such as dark-web forums, leak repositories, and breach intelligence platforms can reveal whether firewall technologies, configurations, or exposed network services are being discussed or actively targeted by adversaries. Such intelligence provides valuable contextual insight that extends beyond mere confirmation of control existence, enabling auditors to assess real-world exposure and inherited risk, in line with the Anti-Sheriff cybersecurity auditing philosophy.

Over time, continued reliance on this approach (binary check) adversely affects business continuity and operational stability, when latent control weaknesses, including zero-day attacks and internal lateral movement, remain undetected. These weaknesses can result in security incidents that disrupt core business processes and potentially affect revenue generation, despite the organization appearing compliant under conventional audit practices.

The proposed approach provides a foundational baseline for evolving cybersecurity audits from binary compliance verification toward risk-based evaluation. This transition enables the audit process to account for additional influential factors, including intelligence derived from public sources and structured human judgment. A critical evaluation of the

proposed model is, therefore, required before identifying areas for future research and concluding the study.

5.4. Model Critical Evaluation

As asserted by Hossain et al. [32], adopting intelligence must account for human societal considerations, including human judgment and model explainability; Muthukrishnan et al. [47] similarly dwell on the centrality of human-in-the-loop approaches. In the present study, the proposed model integrates intelligence risk indicators capabilities with human judgment to enhance the effectiveness of technical cybersecurity controls and audit processes for compliance and business-strategy alignment. Debate persists over the quantification of cybersecurity risk; however, the proposed model introduces a scoring mechanism that supports the quantitative assessment of control maturity and the overall cybersecurity audit process maturity, based on both human and intelligence risk indicators. This approach provides a bounded, explainable, and risk-based framework that clarifies the relationship between human expertise and intelligence risk indicators collaboration in strengthening cybersecurity control postures.

As demonstrated in the experimental evaluation, a key strength of the proposed model lies in its dual-lens assessment of technical controls and compliance auditing against defined standards and internal organizational policies. By integrating technical control evaluation with audit oversight, the model supports a comprehensive assessment of cybersecurity posture. The model also incorporates human factors, reinforcing the Anti-Sheriff audit philosophy. While the model demonstrates the capacity to quantify real-world control effectiveness beyond checklist-based compliance, a critical evaluation remains necessary to assess its robustness, validity, and limitations, as summarized in Table 10.

Table 10. Model critical evaluation summary.

Evaluation Criteria	Rational	Results	Explanation
Alignment with existing cybersecurity standards and models	The proposed model should align logically with international standards and benchmarks, such as CIS, NIST CSF, and ISO 27001.	✓	The study explicitly references internationally recognized standards, including CIS and NIST CSF. Cybersecurity controls adopted in the model are derived from the NIST CSF to ensure that the proposed model is not positioned as a replacement for existing standards, but rather as a complementary and augmentative auditing framework.
Dependability of data sources	The data source used should be reliable and easily accessible to support study repeatability and future research.	–	The empirical demonstration relied on a controlled experimental environment, which may limit ecological validity. In an ideal world, a simulated environment with more than one server can provide a more realistic representation of the perception behind the proposed model.
Human judgment–centric design	To evaluate the proportional contribution of human judgment toward improving audit outcomes.	✓	The model explicitly incorporates human-centered decision-making, demonstrating that expert judgment plays a critical role in shaping the final risk score, particularly in interpreting governance maturity, contextual risk, and residual exposure.
Scalability and automation potential	To determine whether the model can be generalized, scaled, or automated for large-scale cybersecurity audits.	–	The proposed model automates most analytical and aggregation steps; however, the binary compliance verification of control existence was conducted manually. Additional automation—particularly for control discovery and configuration assessment, thus, would further improve scalability and operational efficiency.
Explainability, interpretability, and transparency	To evaluate the clarity and accessibility of model outputs for both technical and non-technical stakeholders.	✓	The model was designed and presented in a manner that supports transparent, explainable, and interpretable outputs, enabling understanding by auditors, management, and non-technical decision-makers.
Empirical applicability and validation	To assess whether the model can be applied meaningfully to real-world audit or incident scenarios.	✓	A structured fictional case scenario was used to empirically demonstrate the applicability of the model, simulating real-world cybersecurity audit conditions and validating the feasibility of the proposed approach.

For clarity, fully satisfied evaluation criteria are marked with a tick (✓), partially satisfied criteria are indicated with a dash (–), and criteria that are not satisfied are denoted by a cross (×).

Traditionally, a comprehensive literature review is presented at the outset of a study, prior to articulating the research contribution. However, as previously noted, this study is not a stand-alone literature review, and the inclusion of a dedicated, exhaustive review section was therefore deemed out of scope. At this stage, the authors have demonstrated the core contribution of the proposed model and its distinction from traditional cybersecurity binary compliance-check approaches. Nevertheless, before concluding the study, it is essential to examine related work more closely to contextualize the contribution and demonstrate the distinctiveness of the proposed approach. Accordingly, as presented in Table 11, a comparative analysis between the proposed model and existing approaches is key.

Table 11. Comparative analysis of related work and the proposed Anti-Sheriff Cybersecurity Audit Model.

Ref.	Study Approach	Primary Focus	Key Characteristics	Comparison with the "Anti-Sheriff Model"
Mohammad et al. [19]	The authors proposed an AFRA Framework (Modular AI Integration)	AI-augmented financial ratio analysis for early warning and monitoring using transactional integrity.	Blockchain-based tamper-evident logs for integrity maintenance.	AFRA is metric-centric and focused on financial ratios for continuous monitoring. In contrast, the Anti-Sheriff Cybersecurity Audit Model is governance-centric, assessing multi-dimensional cybersecurity maturity (technical, operational, and organizational) rather than relying on quantitative ratio thresholds alone.
Muhammad et al. [48]	L-XAIDS Framework (LIME-based XAI)	Improving explainability in IDSs	Integration of LIME and ELI5; local and global explanations for security alerts	The proposed L-XAIDS addresses technical transparency by explaining AI decisions. The Anti-Sheriff Cybersecurity Audit Model extends this by embedding explainable outputs within a broader audit philosophy that supports structured human judgment and risk-informed assurance for both technical and non technical personel.
Zastempowski et al. [20]	Systematic Literature Review (SLR)	Reshaping IT audit practices through ML and AI.	Identification of frameworks that focus on APT detection and risk management for enhanced IT auditing processes.	This work is exploratory, identifying gaps and trends in the field. The Anti-Sheriff Cybersecurity Audit Model is prescriptive, proposing a concrete audit model and scoring mechanism to capture residual cybersecurity risk.
Al-Hashimi et al. [49]	GenAI-SSDLC (Generative AI Framework)	Enhancing security across the software development life cycle	GenAI-driven threat modeling, automated compliance checks, and security-by-design across SDLC phases	GenAI-SSDLC automates traditional compliance checklists during development. The Anti-Sheriff Cybersecurity Audit Model redefines compliance by replacing static checklist validation with adaptive, intelligence-informed maturity assessments at the audit level.
Rout et al. [10]	FSEGM Model (Feature Selection & Ensemble	Adaptive cloud security and zero-day threat detection.	Bayesian network fusion for dimensionality reduction in cybersecurity threats within the cloud environments.	This model prioritizes predictive accuracy and detection performance. The Anti-Sheriff Cybersecurity Audit Model prioritises assurance relevance, shifting focus from binary detection outcomes to evaluating organizational control effectiveness and governance posture.
Guptta et al. [50]	Hybrid Feature-Based Phishing Detection	Real-time phishing website detection	Predictive classifiers for detecting zero-hour attack focus.	This represents a specific technical enforcement control. The Anti-Sheriff Cybersecurity Audit Model differs by providing a holistic auditing framework to evaluate the effectiveness and governance maturity of multiple such controls collectively.

As demonstrated in Table 11, the comparative analysis further highlights that, while existing studies and frameworks make significant advances in areas such as AI-driven detection, explainability, continuous monitoring, and automated compliance, they remain largely solution-centric and narrowly scoped to specific technical or operational objectives. The proposed Anti-Sheriff Cybersecurity Audit Model is one of its kind that is positioned as a governance-aware and assurance-oriented auditing model that integrates such intelligence outputs within a unified, risk-informed audit process whilst ensuring that business needs at the organizational level are realized. Most of the available approaches from the literature as depicted in Table 1, are primarily aimed at improving the performance, accuracy, or transparency of individual security functions, such as intrusion detection, threat prediction, or policy enforcement, and are seldom designed with cybersecurity auditing, assurance, or governance decision-making as their primary objective. Notably, they have a uniform perceived outcome, wherein their outputs are often treated as standalone technical results rather than as structured evidence that can be systematically interpreted, justified, and relied upon within an audit context.

In contrast, the proposed Anti-Sheriff Cybersecurity Audit Model is explicitly designed as an audit-first framework, rather than a detection- or control-first solution. Its distinguishing contribution lies in its ability to translate heterogeneous intelligence outputs into auditable, explainable, and governance-aligned insights through a layered integration of binary compliance verification, intelligence-supported risk indicators, and structured human judgment. Rather than replacing existing tools or metrics, the model provides a unifying audit logic that contextualizes their outputs within organizational risk appetite, control maturity, and accountability structures. This governance-centric orientation enables the model to assess not only whether controls exist or detect threats, but whether they are effective, defensible, and aligned with business objectives under dynamic threat conditions.

Furthermore, as a means to address residual risk that might remain after the implementation of cybersecurity controls, the Anti-Sheriff Cybersecurity Audit Model looks beyond the general technical risks lens. The proposed model departs from check list by reframing cybersecurity audits as an enablement and assurance activity rather than a policing exercise. Further to that, the model enhances insights through human judgment as a formal decision layer and treats intelligence as a supporting, rather than deterministic, mechanism. The model addresses critical concerns related to explainability, accountability, and trust that are often overlooked in technically focused frameworks. This integrated perspective positions the proposed model as one that bridges the gap between technological adoption within cybersecurity capabilities and governance-oriented cybersecurity auditing, thereby offering a distinctive contribution that extends beyond existing solution-specific or compliance-automation models.

Whilst the authors strongly believe that the proposed model can be used as a foundational reference from which a shift from binary check to a more risk-based approach can be built or improved on. This study is not free from shortcomings; as such, the next section expands on the study limitations and further directions that future studies can explore.

6. Study Limitations and Future Work

The challenges arising from the ongoing evolution of ICT and technological advancement cannot be resolved by a single study. Responding to these challenges requires more integrated, collaborative research across cybersecurity and related technological domains.

6.1. Study Limitations

A key limitation of the present study relates to its defined scope. As demonstrated by Muyambo et al. [51], in order to ensure that a study does not diverge from the main

objective, a particular scope needs to be defined and adhered to. The present study's scope did not entail a standalone systematic review. A second limitation concerns using fictional or simulated scenario data; while such data adequately support experimental validation and PoC demonstration, they may not fully reflect the complexity and unpredictability of real-world environments. The robustness of the proposed approach could be strengthened by applying the model in operational organizational contexts or by using data derived from historical cybersecurity audit engagements. The other limitation was demonstrated on the experimental setup; the case scenario used only covers up to the second part of the proposed model, and the last test was not demonstrated. These shortcomings are left to be addressed in future research avenues, as pointed out next.

6.2. Future Direction

Future studies can expand the scope beyond technical cybersecurity control assessments to examine cybersecurity governance risks and the role of modern technologies, including AI, in mitigating such risks. Future work may also adopt a broader range of research methodologies, including qualitative approaches, such as interviews and questionnaires with cybersecurity experts, to assess the practical applicability of AI in advancing cybersecurity practice. A mixed-method design could further enrich understanding by integrating empirical technical evaluation with practitioner perspectives. Future researchers should define different case scenarios, compare results under different conditions, and observe how the model will respond in such diverse contexts. Given the exploratory and design-oriented nature of the current study, a comprehensive "state-of-the-art" literature review was not presented as a standalone section, due to the scope of the study and the length constraints of the journal. Instead, the relevant gaps and insights from the literature were synthesized within the study motivation and analysis sections. The authors therefore recommend that future research further explore developments in this area to continuously assess emerging opportunities and evolving gaps in cybersecurity auditing. The need for a standalone systematic literature review of modern technologies such as AI was also noted by Kaur et al. [39] and Birksted et al. [52].

With the study's limitations and future research directions defined, the present study concludes.

7. Conclusions

This study was motivated by the persistent gap between rapidly evolving, intelligence-driven cybersecurity threats and auditing practices that remain predominantly compliance-oriented and retrospective in nature. The authors have observed that the rapidly increasing rate of modern and sophisticated cyber threats requires a rethink in the way cybersecurity controls are tested. Without downplaying the role of the numerous standards, controls, and frameworks that exist, the authors have particularly noted that the available approaches largely focus on confirming the presence of controls rather than evaluating their effectiveness under dynamic threat conditions. In a quest to address the identified rigid challenges of conducting cybersecurity assessments through sound auditing, the present study therefore presents a model, the "Anti-Sheriff Approach," which is primarily focused on reframing cybersecurity auditing from a "sheriff-style" enforcement exercise into a risk-informed, intelligence-supported assurance process. The proposed approach integrates external threat intelligence, structured human judgment, and governance considerations for a sound cybersecurity audit outcome. The proposed approach provides a foundation for future research to empirically validate the model across diverse organizational contexts, refine risk-weighting mechanisms, and explore automation pathways that support continuous, scalable, and explainable cybersecurity auditing in complex digital ecosystems.

The findings from the case study demonstration concretize that binary cybersecurity confirmation exercises can be misleading. As observed, stakeholders may be presented with an inaccurate cybersecurity posture and become overly comfortable based on less-informed cybersecurity auditing outcomes. The proposed model moves beyond confirmation by combining automated intelligence inputs with structured expert oversight, thereby directly addressing the limitations of traditional binary audit methods and enabling deeper analysis, improved contextual awareness, and more adaptive audit outcomes. As cybersecurity threats continue to increase in complexity and sophistication, such an approach becomes essential not only for safeguarding information exchange but also for sustaining stakeholder confidence in digital transformation initiatives. While the adoption of modern technologies such as AI within cybersecurity is promising, there remains a strong need to incorporate intelligence aligned with overall business objectives and to move beyond purely technical assessments. Adopting hybrid and flexible cybersecurity auditing approaches, as presented in the study, therefore, serves as a key reference point in combating modern cybersecurity threats.

8. Disclaimer

The authors acknowledge the limited use of AI-generated content in the study titled "An Anti-Sheriff Cybersecurity Audit Model: From Compliance Checklists to Intelligence-Supported Cyber Risk Auditing." ChatGPT 5.2 was used to improve the readability of selected concepts; all such content was subsequently reviewed, reworded, and edited to align with the study's objectives and scholarly standards. Grammarly was used to identify spelling and grammatical issues before submission to a professional language editor.

Author Contributions: Conceptualization, N.R. and H.S.V.; methodology, N.R.; validation, N.R. and H.S.V.; formal analysis, N.R.; investigation, N.R.; writing—original draft preparation, N.R.; writing—review and editing, N.R. and H.S.V.; visualization, N.R.; supervision, H.S.V.; project administration, N.R.; funding acquisition, H.S.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial intelligence
APT	Advanced persistent threats
CCM	Continuous control monitoring
CIA	Confidentiality, integrity, and availability
CIS	Center for Internet Security
CISA	Certified Information Systems Auditor
CMM	Capability Maturity Model
CSF	Cybersecurity Framework
CVE	Common vulnerabilities and exposures
DLP	Data loss prevention
DR	Disaster recovery
DSR	Design science research
DSRM	Design science research methodology
EDR	Endpoint detection and response

EPSS	Exploit prediction scoring system
ICT	Information and communication technology
IDS	Intrusion detection systems
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IR	Incident response
IS	Information systems
ISACA	Information Systems Audit and Control Association
KPI	Key performance indicators
MFA	Multi-factor authentication
MI	Material irregularities
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSINT	Open-source intelligence
PoC	Proof-of-concept
POPIA	Protection of Personal Information Act
PR	Pull requests
RPO	Recovery point objective
RTO	Recovery time objective
SIEM	Security information and event management
SME	Small and medium-sized enterprises
SOAR	Security orchestration, automation, and response
UEBA	User and entity behavior analytics

References

1. Kumawat, H.; Meena, G. Characterization, detection and Mitigation of Low-Rate DoS attack. In *ICTCS '14: Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*; Association for Computing Machinery: New York, NY, USA, 2014. [CrossRef]
2. Rananga, N.; Venter, H.S. Mobile Cloud Computing Adoption Model as a Feasible Response to Countries' Lockdown as a Result of the COVID-19 Outbreak and beyond. In *Proceedings of the 2020 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*; IEEE: New York, NY, USA, 2020; pp. 61–66. [CrossRef]
3. Singh, K.; Best, P. Auditing during a pandemic—Can continuous controls monitoring (CCM) address challenges facing internal audit departments? *Pacific Account. Rev.* **2023**, *35*, 727–745. [CrossRef]
4. Pirbhulal, S.; Chockalingam, S.; Shukla, A.; Abie, H. *IoT Cybersecurity in 5G and Beyond: A Systematic Literature Review*; Springer: Berlin/Heidelberg, Germany, 2024.
5. Chen, M.; Liu, F.; Liang, D.; Zhong, S.; Li, Y. Entity Recognition for Power Equipment Data Based on Optional Word Vectors and Feature Fusion. *IEEE Access* **2025**, *13*, 143767–143780. [CrossRef]
6. Mohawesh, R.; Ottom, M.A.; Salameh, H.B. A data-driven risk assessment of cybersecurity challenges posed by generative AI. *Decis. Anal. J.* **2025**, *15*, 100580. [CrossRef]
7. Bibri, S.E.; Huang, J. Generative AI of things for sustainable smart cities: Synergizing cognitive augmentation, resource efficiency, network traffic, cybersecurity, and anomaly detection for environmental performance. *Sustain. Cities Soc.* **2025**, *133*, 106826. [CrossRef]
8. Pinto, B.S.; Cioffi, L.; Esposito, F. Third-party Cloud Risk Management. In *Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience (CSR)*; IEEE: New York, NY, USA, 2024; pp. 445–451. [CrossRef]
9. Mutalib, N.H.A.; Sabri, A.Q.M.; Wahab, A.W.A.; Abdullah, E.R.M.F.; AlDahoul, N. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: A review. *Artif. Intell. Rev.* **2024**, *57*, 297. [CrossRef]
10. Rout, C.; Sethi, S.; Badajena, J.C.; Sahoo, R.K. FSEGM: Feature selection and ensemble generative model for adaptive cloud security. *J. Cloud Comput.* **2026**, *15*, 6. [CrossRef]
11. Sulistyowati, D.; Handayani, F.; Suryanto, Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *Int. J. Inform. Vis.* **2020**, *4*, 225–230. [CrossRef]
12. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 698–736. [CrossRef]
13. Zadeh, A.; Lavine, B.; Zolbanin, H.; Hopkins, D. A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decis. Anal. J.* **2023**, *9*, 100328. [CrossRef]

14. Agrafiotis, I.; Nurse, J.R.C.; Goldsmith, M.; Creese, S.; Upton, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J. Cybersecur.* **2018**, *4*, tyy006. [CrossRef]
15. Parmar, M.; Miles, A. Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2.0 and EU Standards. In *Proceedings of the 2024 Security for Space Systems (3S)*; IEEE: New York, NY, USA, 2024; pp. 1–7. [CrossRef]
16. Andrade, R.O.; Yoo, S.G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *J. Inf. Secur. Appl.* **2019**, *48*, 102352. [CrossRef]
17. Mahar, F.; Ali, S.I.; Jumani, A.K.; Khan, M.O. ERP System Implementation: Planning, Management, and Administrative Issues. *Indian J. Sci. Technol.* **2020**, *13*, 106–122. [CrossRef]
18. Alenezi, A.; Atlam, H.F.; Wills, G.B. Experts reviews of a cloud forensic readiness framework for organizations. *J. Cloud Comput.* **2019**, *8*, 11. [CrossRef]
19. Nachouki, M. AI-Augmented Financial Ratio Analysis for Early Warning, Monitoring, and Assurance. In *Proceedings of the 2025 8th International Conference on Signal Processing and Information Security (ICSPIS)*; IEEE: New York, NY, USA, 2025; pp. 1–5. [CrossRef]
20. Pycka, M.; Zastempowski, M. Machine learning and artificial intelligence techniques adopted for IT audit. *Management* **2025**, *29*, 65–87. [CrossRef]
21. Muringani, J.; Noll, J.; Kimambo, C.; Mansour, W.A.; Mapitsa, C.B.; Roberson, J.; Karanja, J.; Orbach, R. Evidence and Gap on Mobile Internet Usage in Sub-Saharan Africa and South Asia. In *Proceedings of the 2025 IST-Africa Conference (IST-Africa)*; IEEE: New York, NY, USA, 2025; pp. 1–10. [CrossRef]
22. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining Cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]
23. Do Xuan, C.; Huong, D. A new approach for APT malware detection based on deep graph network for endpoint systems. *Appl. Intell.* **2022**, *52*, 14005–14024. [CrossRef]
24. Sánchez-García, I.D.; Feliu Gilabert, T.S.; Calvo-Manzano, J.A. Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. *Comput. Secur.* **2023**, *128*, 103170. [CrossRef]
25. Cooke, I. IS Audit Basics: Auditing Cybersecurity. 2019. Available online: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/is-audit-basics-auditing-cybersecurity (accessed on 31 July 2024).
26. NIST Computer Security Resource Center. Available online: https://csrc.nist.gov/glossary/term/cybersecurity (accessed on 12 August 2024).
27. Cannon, D.L. *CISA Certified Information Systems Auditor™ Study Guide*; Wiley & Sons: Hoboken, NJ, USA, 2015; Volume 1.
28. Al-Matari, O.M.M.; Helal, I.M.A.; Mazen, S.A.; Elhennawy, S. Integrated framework for cybersecurity auditing. *Inf. Secur. J.* **2021**, *30*, 189–204. [CrossRef]
29. Al-Dhaqm, A.; Razak, S.A.; Siddique, K.; Ikuesan, R.A.; Kebande, V.R. Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access* **2020**, *8*, 145018–145032. [CrossRef]
30. vom Brocke, J.; Hevner, A.; Maedche, A. Introduction to Design Science Research. In *Design Science Research. Cases*; Springer: Cham, Switzerland, 2020; pp. 1–13. [CrossRef]
31. Venable, J.; Pries-Heje, J.; Baskerville, R. A comprehensive framework for evaluation in design science research. In *Design Science Research in Information Systems. Advances in Theory and Practice*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7286, pp. 423–438. [CrossRef]
32. Hossain, M.J.; Alam, K.; Monir, M.F.; Hoque, M.M.; Ahmed, T. Explainable AI Meets Synthetic Data: A Deep Learning Framework for Detecting Network Intrusion in NextG Network Infrastructure. *IEEE Access* **2025**, *13*, 114979–115001. [CrossRef]
33. Dambe, S.; Gochhait, S.; Ray, S. The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In *Proceedings of the 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)*; IEEE: New York, NY, USA, 2023; pp. 88–93. [CrossRef]
34. Bartwal, U.; Mukhopadhyay, S.; Negi, R.; Shukla, S. Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. In *Proceedings of the 2022 IEEE Conference on Dependable and Secure Computing (DSC)*; IEEE: New York, NY, USA, 2022; pp. 1–8. [CrossRef]
35. Bashofi, I.; Salman, M. Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. In *Proceedings of the 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*; IEEE: New York, NY, USA, 2022; pp. 58–62. [CrossRef]
36. Wei, W.; Liu, L. Trustworthy Distributed AI Systems: Robustness, Privacy, and Governance. *ACM Comput. Surv.* **2025**, *57*, 143. [CrossRef]
37. Malatji, M. Augmented Intelligence Framework for Human—Artificial Intelligence Teaming in Cybersecurity. *Human-Centric Intell. Syst.* **2025**, *5*, 151–180. [CrossRef]
38. Michael, K.; Abbas, R.; Roussos, G. AI in Cybersecurity: The Paradox. *IEEE Trans. Technol. Soc.* **2023**, *4*, 104–109. [CrossRef]
39. Kaur, R.; Gabrijelčič, D.; Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Inf. Fusion* **2023**, *97*, 101804. [CrossRef]

40. Carey, M.J.; Jin, J. *Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World*; John Wiley & Sons: Hoboken, NJ, USA, 2019; Volume 11.
41. Adler, R.M. A dynamic capability maturity model for improving cyber security. In *Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security (HST)*; IEEE: New York, NY, USA, 2013; pp. 230–235. [CrossRef]
42. Cai, M.; Yang, J.; Gao, J.; Lee, Y.J. Matryoshka Multimodal Models. *arXiv* **2024**, arXiv:2405.17430. [CrossRef]
43. Arora, S.; Dalal, S. Ddos attacks simulation in cloud computing environment. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *9*, 414–417. [CrossRef]
44. Sanchez-Paniagua, M.; Fernandez, E.F.; Alegre, E.; Al-Nabki, W.; Gonzalez-Castro, V. Phishing URL Detection: A Real-Case Scenario Through Login URLs. *IEEE Access* **2022**, *10*, 42949–42960. [CrossRef]
45. Jacobs, J.; Romanosky, S.; Edwards, B.; Adjerid, I.; Roytman, M. Exploit Prediction Scoring System (EPSS). *Digit. Threat. Res. Pract.* **2021**, *2*, 20. [CrossRef]
46. Cosentino, V.; Izquierdo, J.L.C.; Cabot, J. A Systematic Mapping Study of Software Development with GitHub. *IEEE Access* **2017**, *5*, 7173–7192. [CrossRef]
47. Muthukrishnan, H. A Policy-Aware Framework for Data Masking: Secure Integration of Applications and Artificial Intelligence in Healthcare and Financial Services. In *Proceedings of the 2025 International Seminar on Application for Technology of Information and Communication (iSemantic)*; IEEE: New York, NY, USA, 2025; pp. 468–473. [CrossRef]
48. Muhammad, A.E.; Yow, K.C.; Bačanin-Džakula, N.; Khan, M.A. L-xaids: A LIME-based eXplainable AI framework for intrusion detection systems. *Clust. Comput.* **2025**, *28*, 654. [CrossRef]
49. Al-Hashimi, H.A.; Khan, R.A.; Alwageed, H.S.; Algarni, A.M.; Ayouni, S.; Almagrabi, A.O. Exploring the role of generative AI in enhancing cybersecurity in software development life cycle. *Array* **2025**, *28*, 100509. [CrossRef]
50. Das Guptta, S.; Shahriar, K.T.; Alqahtani, H.; Alsalman, D.; Sarker, I.H. Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques. *Ann. Data Sci.* **2024**, *11*, 217–242. [CrossRef]
51. Muyambo, E.; Baror, S.; Makura, S. Digital Forensic-Ready Voting Model. *Indones. J. Comput. Sci.* **2025**, *14*, 10219–10237. [CrossRef]
52. Birkstedt, T.; Minkkinen, M.; Tandon, A.; Mäntymäki, M. AI governance: Themes, knowledge gaps and future agendas. *Internet Res.* **2023**, *33*, 133–167. [CrossRef]