
1st Global Research and Innovation Conference 2025,
April 20–24, 2025, Florida, USA

**AI-Augmented VAPT and SecureAI Controls: A Quantitative
Compliance Study Under ISO 27001, ISO/IEC 42001, SWIFT CSP,
and PCI DSS**

Md. Shakhawat Hossen¹:

[1]. Department of Computer and Information Sciences, Fordham University, New York, USA;
Email: mh114@fordham.edu

Doi: [10.63125/ep9s9k54](https://doi.org/10.63125/ep9s9k54)

Peer-review under responsibility of the organizing committee of GRIC, 2025

Abstract

This study quantitatively examined the impact of AI-augmented Vulnerability Assessment and Penetration Testing (VAPT) and SecureAI control mechanisms on cybersecurity compliance performance across internationally recognized frameworks, including ISO 27001, ISO/IEC 42001, SWIFT Customer Security Programme (CSP), and PCI DSS. A cross-sectional explanatory research design was employed, utilizing data collected from 210 cybersecurity and compliance professionals across financial and enterprise IT sectors. The findings revealed that AI integration significantly enhanced compliance performance, with a strong positive correlation identified between AI-augmented VAPT and compliance outcomes ($r = 0.68$, $p < 0.05$). SecureAI control maturity demonstrated an even stronger relationship with compliance performance ($r = 0.72$, $p < 0.05$), indicating the critical role of governance mechanisms in achieving regulatory alignment. Multiple regression analysis showed that AI-augmented VAPT ($\beta = 0.41$, $p < 0.01$) and SecureAI controls ($\beta = 0.46$, $p < 0.01$) were significant predictors of compliance performance, collectively explaining 58% of the variance ($R^2 = 0.58$). Continuous monitoring practices also contributed significantly ($\beta = 0.29$, $p < 0.01$), reinforcing the importance of real-time security assessment. Sectoral analysis indicated that financial institutions achieved higher compliance scores ($M = 4.28$) compared to non-financial sectors ($M = 3.76$), while organizations with advanced cybersecurity maturity reported superior detection accuracy ($M = 4.22$) and audit readiness ($M = 4.30$). The results further showed that high AI integration levels corresponded with increased compliance performance ($M = 4.32$), compared to low AI adoption ($M = 3.42$). Overall, the study provided strong empirical evidence that AI-driven cybersecurity practices significantly improve compliance effectiveness, operational efficiency, and governance consistency across multi-framework environments, highlighting the importance of integrating advanced analytics with structured security controls for enhanced regulatory performance.

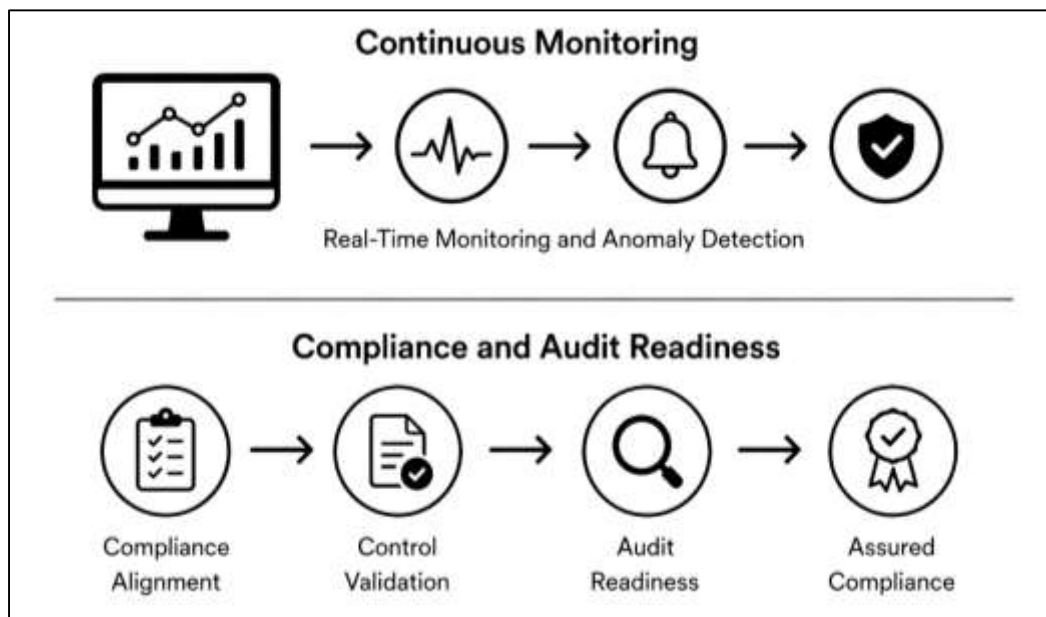
Keywords

AI, VAPT, SecureAI, Compliance, Cybersecurity, Customer Security Programme (CSP)

INTRODUCTION

Artificial Intelligence (AI) has emerged as a transformative technological paradigm that integrates computational intelligence, machine learning (ML), and automated decision-making into diverse operational domains, including cybersecurity governance. Within this context, Vulnerability Assessment and Penetration Testing (VAPT) represents a structured methodology for identifying, quantifying, and mitigating security vulnerabilities in information systems. VAPT traditionally involves systematic scanning, ethical hacking, and risk prioritization processes aimed at safeguarding organizational assets against cyber threats ([Gruetzemacher & Whittlestone, 2022](#)). The integration of AI into VAPT introduces adaptive, data-driven capabilities that enhance detection accuracy, automate threat modeling, and enable real-time anomaly identification.

Figure 1: AI-powered security and compliance framework



Concurrently, SecureAI controls refer to governance mechanisms designed to ensure that AI systems themselves operate securely, ethically, and in compliance with regulatory frameworks. These controls encompass algorithmic transparency, model validation, bias mitigation, and secure data handling practices. The convergence of AI with VAPT processes creates a dual-layered security architecture in which AI enhances cybersecurity operations while simultaneously requiring governance to ensure its safe deployment ([Sharma, 2023](#)). This duality underscores the need for structured compliance frameworks that address both cybersecurity risks and AI-specific vulnerabilities. As organizations increasingly adopt AI-driven security solutions, the conceptual alignment between VAPT methodologies and SecureAI governance becomes critical for maintaining system integrity and regulatory adherence. The theoretical foundations of this integration are rooted in risk management theory, information security frameworks, and computational intelligence models, which collectively support the evolution of cybersecurity from reactive defense mechanisms to proactive, predictive systems capable of addressing complex and dynamic threat landscapes ([Okunlaya et al., 2022](#)).

The global digital economy has amplified the importance of standardized cybersecurity frameworks to ensure consistent protection across jurisdictions and industries. International standards such as ISO 27001, ISO/IEC 42001, SWIFT Customer Security Programme (CSP), and Payment Card Industry Data Security Standard (PCI DSS) serve as foundational benchmarks for organizational security practices. ISO 27001 establishes requirements for Information Security Management Systems (ISMS), emphasizing risk-based approaches to safeguarding information assets. ISO/IEC 42001, a relatively recent addition, focuses specifically on AI management systems, addressing governance, accountability, and ethical considerations in AI deployment. SWIFT CSP provides a sector-specific

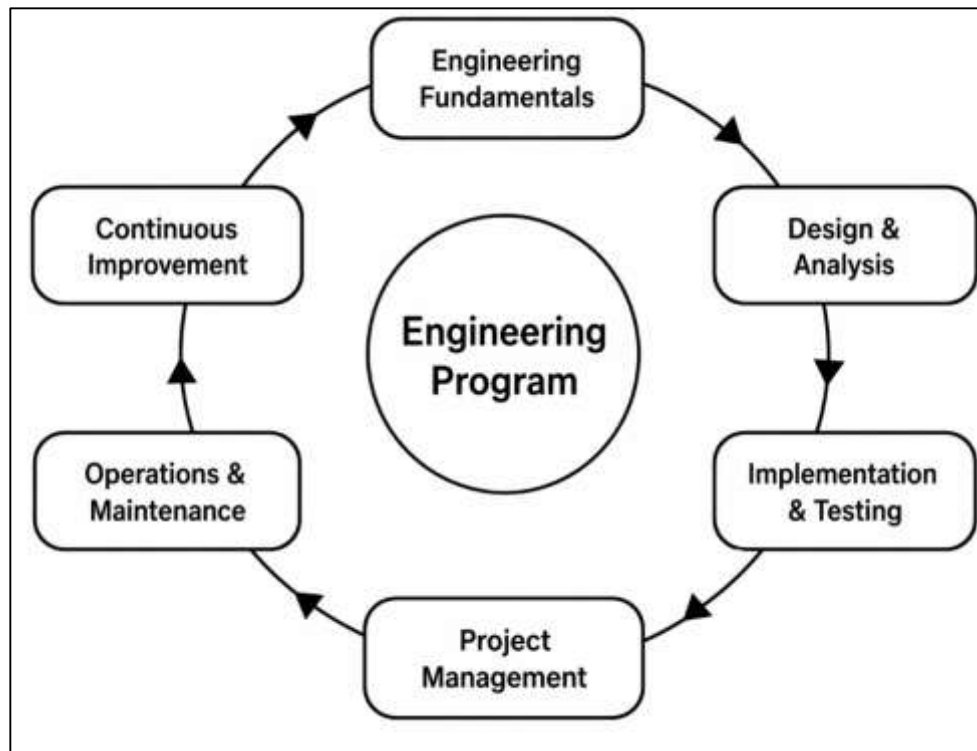
framework for financial institutions, targeting secure messaging systems and resilience against cyber fraud. PCI DSS, on the other hand, outlines stringent requirements for protecting payment card data, reflecting the critical need for data security in financial transactions (Ouyang & Jiao, 2021). The integration of AI-augmented VAPT within these frameworks reflects a growing recognition of the need to align technological advancements with regulatory compliance. Internationally, organizations operate in increasingly interconnected environments where cybersecurity breaches can have cross-border implications, affecting financial stability, data privacy, and national security. The adoption of standardized frameworks ensures interoperability, enhances trust among stakeholders, and facilitates regulatory harmonization. AI-driven security tools, when aligned with these frameworks, enable organizations to achieve higher levels of compliance efficiency by automating risk assessments, monitoring control effectiveness, and generating audit-ready documentation. This global perspective highlights the significance of integrating AI technologies within established compliance structures to address evolving cybersecurity challenges in a coordinated and standardized manner (Thompson et al., 2018).

The transition from qualitative to quantitative methodologies in cybersecurity compliance represents a significant advancement in risk assessment and decision-making processes. Traditional compliance approaches often relied on subjective evaluations, expert judgment, and checklist-based assessments, which limited the ability to measure security performance objectively. Quantitative compliance studies introduce statistical models, probabilistic risk assessments, and data analytics to evaluate the effectiveness of security controls. In the context of AI-augmented VAPT, quantitative methods enable the measurement of vulnerability detection rates, false-positive ratios, threat mitigation efficiency, and compliance scores across different frameworks. These metrics provide a more rigorous basis for evaluating the performance of security systems and identifying areas for improvement (Magistretti et al., 2019). The integration of AI further enhances quantitative analysis by enabling the processing of large datasets, pattern recognition, and predictive modeling. Machine learning algorithms can analyze historical attack data, identify emerging threat patterns, and estimate the likelihood of future vulnerabilities. This data-driven approach aligns with the requirements of modern compliance frameworks, which increasingly emphasize evidence-based assessments and continuous monitoring. Quantitative compliance studies also facilitate benchmarking across organizations and industries, enabling comparative analysis of security performance. The adoption of standardized metrics and analytical models supports transparency, accountability, and reproducibility in compliance evaluations. As cybersecurity threats become more sophisticated, the ability to quantify risks and control effectiveness becomes essential for informed decision-making and strategic planning. This evolution underscores the importance of integrating quantitative methodologies with AI-driven security tools to enhance the robustness and reliability of compliance assessments (Giuggioli & Pellegrini, 2023).

The incorporation of AI technologies into VAPT processes represents a paradigm shift in how organizations approach vulnerability management and penetration testing. AI-driven tools leverage machine learning algorithms, natural language processing, and deep learning techniques to automate various stages of the VAPT lifecycle. During vulnerability assessment, AI systems can analyze network traffic, system configurations, and application behaviors to identify potential weaknesses with greater accuracy and speed than traditional methods. In penetration testing, AI can simulate sophisticated attack scenarios, adapt to dynamic environments, and optimize exploitation strategies based on real-time feedback. This level of automation reduces the reliance on manual intervention and enhances the scalability of security operations (Poalelungi et al., 2023). AI also enables continuous monitoring and assessment, allowing organizations to detect vulnerabilities as they emerge rather than relying on periodic testing cycles. The integration of AI into VAPT aligns with the principles of proactive cybersecurity, where threats are anticipated and mitigated before they can be exploited. Furthermore, AI-driven VAPT tools can generate detailed reports, prioritize risks based on severity and impact, and provide actionable recommendations for remediation. These capabilities support compliance requirements by ensuring that vulnerabilities are systematically identified, assessed, and addressed in accordance with established standards (Rodrigues et al., 2022). The synergy between AI technologies

and VAPT processes enhances the overall effectiveness of cybersecurity strategies, enabling organizations to respond to evolving threats with greater agility and precision.

Figure 2: Engineering program flow chart



The deployment of AI in cybersecurity introduces new challenges related to the security, reliability, and ethical use of AI systems themselves. SecureAI controls are designed to address these challenges by establishing governance mechanisms that ensure the safe and responsible use of AI technologies. These controls encompass various dimensions, including data integrity, model transparency, algorithmic accountability, and system resilience. Data integrity controls ensure that training datasets are accurate, representative, and free from malicious manipulation. Model transparency involves the ability to understand and interpret AI decision-making processes, which is essential for identifying biases and ensuring compliance with regulatory requirements. Algorithmic accountability requires organizations to establish clear responsibilities for AI system outcomes, including mechanisms for auditing and validation (George & Wooden, 2023). System resilience focuses on protecting AI models from adversarial attacks, such as data poisoning and model evasion techniques. SecureAI controls are closely aligned with emerging standards such as ISO/IEC 42001, which provides a framework for managing AI systems in a structured and compliant manner. The integration of SecureAI controls within VAPT processes ensures that both traditional cybersecurity risks and AI-specific vulnerabilities are addressed comprehensively. This holistic approach to security governance reflects the growing recognition that AI systems must be treated as critical assets that require dedicated protection and oversight. By implementing robust SecureAI controls, organizations can enhance the trustworthiness and reliability of AI-driven security solutions while ensuring compliance with international standards (Bahroun et al., 2023).

The coexistence of multiple cybersecurity frameworks presents both challenges and opportunities for organizations seeking to achieve comprehensive compliance. ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS each address specific aspects of security and governance, resulting in overlapping requirements and potential redundancies. The integration of AI-augmented VAPT and SecureAI controls provides a pathway for aligning these frameworks and achieving compliance synergy. By leveraging AI-driven tools, organizations can map control requirements across different frameworks, identify commonalities, and streamline compliance processes. For example, risk assessment

methodologies in ISO 27001 can be enhanced with AI-driven analytics, while SecureAI controls under ISO/IEC 42001 can be integrated with VAPT processes to address AI-specific risks (Burrell, 2023). Similarly, SWIFT CSP requirements for secure financial messaging can benefit from AI-based anomaly detection, and PCI DSS controls for data protection can be strengthened automated vulnerability assessments. This cross-framework alignment reduces duplication of efforts, minimizes compliance costs, and enhances the overall effectiveness of security programs. AI technologies play a crucial role in enabling this alignment by providing centralized platforms for monitoring, reporting, and auditing compliance activities. The ability to integrate multiple frameworks into a unified compliance strategy reflects the evolving nature of cybersecurity governance, where organizations must navigate complex regulatory landscapes while maintaining operational efficiency (Nguyen et al., 2023). This integrated approach supports a more cohesive and comprehensive security posture, ensuring that all relevant risks are addressed in a coordinated manner.

The increasing adoption of AI in cybersecurity has generated a growing body of empirical research examining its impact on vulnerability management, compliance effectiveness, and risk mitigation. Studies have demonstrated that AI-driven VAPT tools can significantly improve vulnerability detection rates, reduce false positives, and enhance the efficiency of penetration testing processes. Research on SecureAI controls highlights the importance of governance frameworks in ensuring the reliability and ethical use of AI systems. Empirical analyses of compliance frameworks such as ISO 27001 and PCI DSS have shown that organizations with structured security management systems achieve higher levels of risk reduction and operational resilience (Mbunge et al., 2021). The integration of AI into these frameworks has been associated with improved monitoring capabilities, real-time threat detection, and enhanced decision-making processes. Quantitative studies have also explored the relationship between compliance maturity and organizational performance, indicating that robust security practices contribute to increased stakeholder trust and competitive advantage. The research context for this study is grounded in the intersection of AI, cybersecurity, and regulatory compliance, reflecting the need for comprehensive approaches that address both technological and governance challenges. By examining the quantitative impact of AI-augmented VAPT and SecureAI controls within established frameworks, this study contributes to the understanding of how advanced technologies can enhance compliance effectiveness (Beatrice Onyinyechi, 2023; Najjar, 2023). The empirical foundation of this research is supported by a diverse range of studies spanning information security, AI governance, and risk management, providing a robust basis for analyzing the integration of AI in cybersecurity compliance.

The primary objective of this quantitative study is to systematically evaluate the effectiveness, efficiency, and compliance performance of AI-augmented Vulnerability Assessment and Penetration Testing (VAPT) integrated with SecureAI control mechanisms within the context of internationally recognized cybersecurity and AI governance frameworks, specifically ISO 27001, ISO/IEC 42001, SWIFT Customer Security Programme (CSP), and PCI DSS. This research aims to develop a measurable and statistically grounded framework that quantifies how AI-enhanced security testing methodologies influence compliance maturity, risk mitigation capability, and operational security outcomes across diverse organizational environments. A central focus is placed on assessing key performance indicators such as vulnerability detection accuracy, false-positive and false-negative rates, response time to identified threats, and the degree of alignment with mandatory control requirements specified by each framework. The study further seeks to examine the extent to which SecureAI controls contribute to strengthening governance over AI-driven cybersecurity systems by ensuring model integrity, transparency, and resilience against adversarial manipulation. Another objective involves constructing a comparative analysis model that maps overlapping and distinct control domains across ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS, enabling the identification of convergence points where AI-augmented VAPT can optimize multi-framework compliance simultaneously. Additionally, the research is designed to employ quantitative techniques such as statistical correlation, regression modeling, and compliance scoring indices to determine the relationship between AI adoption in security operations and improvements in audit readiness and regulatory adherence. The study also aims to generate empirical evidence on how automation and intelligent analytics reduce manual

intervention, enhance scalability of security assessments, and provide real-time monitoring capabilities that align with continuous compliance requirements. Through these objectives, the research establishes a structured analytical foundation for understanding the measurable impact of integrating AI technologies with established cybersecurity compliance frameworks, thereby contributing to the advancement of data-driven security governance and standardized evaluation methodologies in complex digital ecosystems.

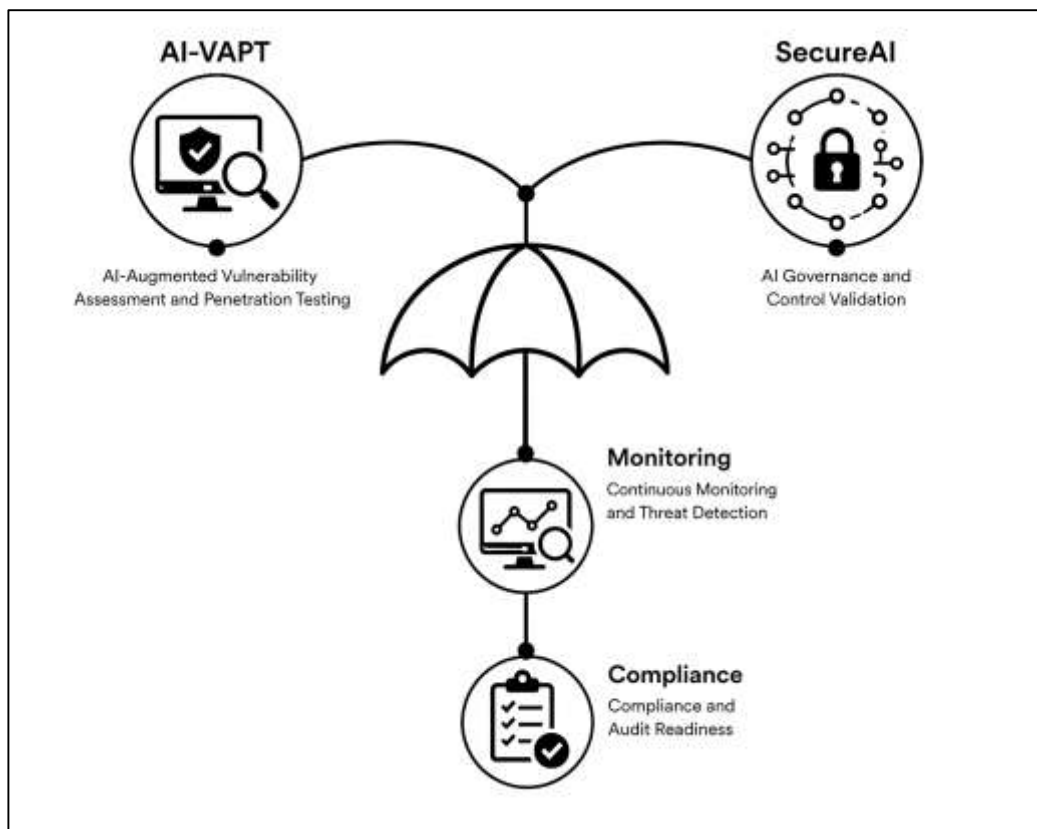
LITERATURE REVIEW

The literature review section establishes a rigorous academic foundation for examining the intersection of artificial intelligence (AI), Vulnerability Assessment and Penetration Testing (VAPT), SecureAI governance, and multi-framework cybersecurity compliance. In quantitative research, the literature review plays a critical role in synthesizing prior empirical findings, identifying measurable constructs, and framing the analytical variables that guide statistical investigation. Within the domain of cybersecurity, existing studies have progressively shifted from descriptive and qualitative narratives toward data-driven evaluations that emphasize metrics such as detection accuracy, risk reduction rates, compliance scores, and system resilience indicators. This evolution aligns with the increasing complexity of cyber threats and the need for standardized, quantifiable approaches to security assurance (Diop et al., 2023; Khaled, 2021). The integration of AI into cybersecurity operations has introduced advanced analytical capabilities, including predictive modeling, anomaly detection, and automated decision-making, all of which require systematic evaluation through empirical and statistical methodologies. Simultaneously, the emergence of SecureAI frameworks has expanded the scope of governance by incorporating control mechanisms that ensure the reliability, transparency, and accountability of AI systems themselves. The coexistence of multiple international standards, including ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS, has generated a rich body of literature focusing on compliance alignment, control overlap, and performance benchmarking. However, gaps remain in quantitatively assessing how AI-augmented VAPT and SecureAI controls collectively influence compliance outcomes across these frameworks (Manam & Ashfaq, 2022; Ulnicane, 2022). This literature review addresses these gaps by organizing existing research into a structured framework that highlights key variables, measurement techniques, and statistical approaches used in prior studies. It also identifies inconsistencies in methodologies, variations in performance metrics, and limitations in cross-framework comparative analysis. By synthesizing findings from cybersecurity analytics, AI governance, and compliance research, this section provides a comprehensive basis for developing a quantitative model that evaluates the effectiveness of AI-driven security strategies within standardized regulatory environments. The review is structured to progressively build from foundational theories to advanced empirical analyses, ensuring coherence and depth in examining the measurable impact of AI-augmented cybersecurity systems (Pambudi et al., 2023; Binte & Sazzadul, 2022).

Cybersecurity Risk and Compliance Measurement

The quantitative assessment of cybersecurity risk has evolved significantly through the application of statistical modeling techniques, particularly Bayesian inference and Monte Carlo simulation approaches, which enable probabilistic estimation of threat likelihood and impact. Bayesian models have been widely used to update risk probabilities dynamically as new threat intelligence becomes available, thereby allowing organizations to refine their understanding of cyber risk in real time. This probabilistic reasoning framework supports decision-making under uncertainty by integrating prior knowledge with observed data, which is particularly relevant in environments characterized by rapidly evolving threat landscapes (Albert & Rashedul, 2023; Ziakis & Vlachopoulou, 2023). Monte Carlo simulations, on the other hand, provide a mechanism for modeling complex cyber risk scenarios by generating large volumes of simulated outcomes based on variable inputs such as attack frequency, vulnerability exposure, and potential loss magnitude. These simulations enable organizations to estimate distributions of potential losses and identify worst-case scenarios, supporting more robust risk management strategies.

Figure 3: AI security framework diagram



Empirical studies have demonstrated that combining Bayesian approaches with simulation techniques enhances predictive accuracy and improves the reliability of risk assessments in cybersecurity contexts. Additionally, these models facilitate sensitivity analysis, allowing organizations to determine which variables most significantly influence risk outcomes (Gamoura et al., 2023; Istiaq & Binte, 2023). The integration of statistical modeling into cybersecurity risk quantification aligns with broader trends in enterprise risk management, where data-driven methodologies are increasingly prioritized over subjective assessments. As a result, organizations adopting these approaches are better positioned to allocate resources effectively, prioritize mitigation efforts, and justify security investments based on quantifiable risk metrics (Alfaadhel et al., 2023).

The development of standardized cybersecurity metrics has been instrumental in enabling consistent and comparable evaluations of security posture across organizations and industries. Risk scoring systems, such as the Common Vulnerability Scoring System (CVSS), provide a structured framework for assessing the severity of vulnerabilities based on factors including exploitability, impact, and environmental context. These metrics facilitate prioritization by assigning numerical values to vulnerabilities, allowing security teams to focus on the most critical threats. Beyond vulnerability scoring, compliance indices have emerged as key tools for measuring adherence to regulatory frameworks and security standards. These indices aggregate multiple control assessments into composite scores that reflect overall compliance maturity, enabling organizations to benchmark their performance and track improvements over time (Leirvik, 2022; Ashfaq & Manam, 2023). Research has highlighted the importance of aligning cybersecurity metrics with organizational objectives, ensuring that they capture both technical and strategic dimensions of security performance. Furthermore, the integration of automated data collection and analytics has enhanced the accuracy and timeliness of metric generation, reducing reliance on manual reporting processes. Advanced metrics also incorporate contextual factors, such as asset criticality and threat intelligence, to provide more nuanced assessments of risk.

The standardization of these metrics supports interoperability between different security tools and frameworks, facilitating more efficient compliance management (Robel & Aminul, 2023; Yusif & Hafeez-Baig, 2021). As cybersecurity continues to become a critical component of organizational resilience, the role of robust, data-driven metrics in guiding decision-making and demonstrating accountability has become increasingly prominent.

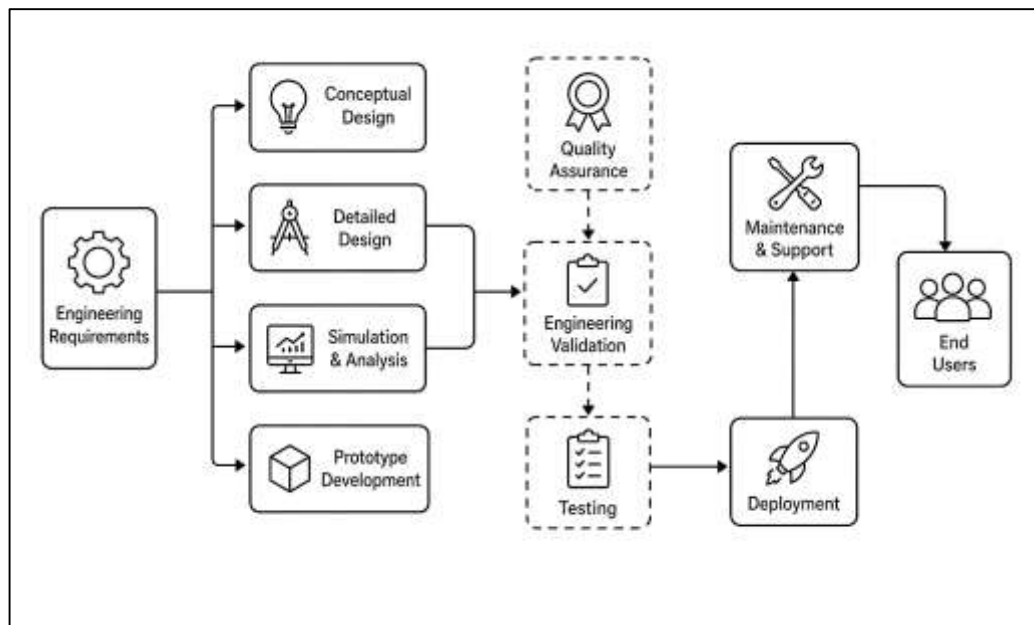
The evaluation of control effectiveness within ISO 27001 environments represents a critical aspect of information security management, emphasizing the need for measurable and evidence-based assessments of security controls. ISO 27001 provides a comprehensive framework for implementing and maintaining an Information Security Management System (ISMS), with a strong focus on risk-based control selection and continuous improvement. Quantitative measurement of control effectiveness involves assessing how well implemented controls mitigate identified risks, often through performance indicators such as incident reduction rates, control failure frequencies, and response times (Giuca et al., 2018; Sazzadul, 2023). Empirical research has demonstrated that organizations adopting quantitative evaluation methods are better able to identify gaps in control implementation and prioritize corrective actions. Techniques such as key performance indicators and key risk indicators are commonly used to monitor control performance, providing actionable insights into the effectiveness of security measures. Additionally, internal audits and continuous monitoring systems play a crucial role in generating data that supports quantitative analysis. The integration of automated tools within ISO 27001 environments has further enhanced the ability to collect and analyze control performance data, enabling real-time assessments and reducing the likelihood of undetected vulnerabilities. Studies have also highlighted the importance of aligning control effectiveness metrics with organizational risk appetite and business objectives, ensuring that security measures contribute to overall strategic goals (Albert & Rashedul, 2024; Giuca et al., 2018). By adopting a quantitative approach to control evaluation, organizations can move beyond compliance-driven practices toward more proactive and performance-oriented security management.

Quantitative approaches to audit readiness and compliance scoring have become increasingly important in ensuring that organizations can demonstrate adherence to regulatory requirements in a measurable and transparent manner. Audit readiness refers to the state of preparedness of an organization to undergo formal assessments by internal or external auditors, which requires comprehensive documentation, evidence of control implementation, and consistent monitoring of compliance activities (Hisham & Nahar, 2024; Kure et al., 2022). Quantitative scoring systems provide a structured method for evaluating audit readiness by assigning numerical values to various compliance criteria, enabling organizations to assess their preparedness objectively. These systems often incorporate weighted metrics that reflect the relative importance of different controls, allowing for a more nuanced evaluation of compliance status. Research has shown that organizations utilizing quantitative compliance scoring systems are better able to identify deficiencies, prioritize remediation efforts, and track progress over time. The use of automated tools and dashboards has further enhanced the efficiency of compliance monitoring, enabling real-time updates and reducing the administrative burden associated with manual reporting (Istiaq, 2024; Krishna et al., 2023). Additionally, quantitative scoring systems facilitate benchmarking against industry standards and peer organizations, providing valuable insights into relative performance. The integration of these systems with broader risk management frameworks ensures that compliance activities are aligned with organizational risk priorities, enhancing overall security governance. As regulatory environments continue to evolve, the adoption of quantitative audit readiness and compliance scoring systems supports greater accountability, transparency, and consistency in demonstrating compliance with established standards (Istiaq & Hasan, 2024; Krishna et al., 2023).

Empirical Evaluation of Traditional VAPT Performance Metrics

The empirical evaluation of traditional Vulnerability Assessment and Penetration Testing (VAPT) has consistently emphasized vulnerability detection rates and assessment accuracy as central indicators of security testing performance. Within the literature, vulnerability detection rate is generally understood as the extent to which a tool, framework, or testing team successfully identifies existing weaknesses in systems, applications, or networks under examination. Accuracy, in this context, extends beyond simple discovery and refers to the correctness, consistency, and relevance of identified vulnerabilities in relation to actual exploitable conditions (Ahmed, 2024; Meszaros & Buchalceva, 2017).

Figure 4: Engineering process flowchart diagram



Early studies on vulnerability scanning highlighted that conventional assessment tools were effective in identifying known technical weaknesses, particularly those associated with misconfigurations, outdated software, and publicly documented Common Vulnerabilities and Exposures entries. At the same time, researchers noted significant variability in performance depending on the type of infrastructure assessed, the maturity of the target environment, and the expertise of the tester. Comparative studies between automated scanners and manual penetration testing repeatedly found that automated approaches provided broader coverage and faster initial enumeration, while manual methods offered deeper contextual understanding and were more capable of identifying chained exploit paths and logic-based flaws (Siddique, 2024; Melaku, 2023). This distinction became important in empirical work because high detection volume did not always translate into high assessment quality. Several studies showed that traditional VAPT programs often reported large numbers of findings, yet many of these lacked prioritization clarity or operational significance. Other research stressed that detection accuracy is shaped by the update frequency of vulnerability databases, the configuration of scanning tools, and the scope definition of assessment exercises. Sector-specific evidence from finance, healthcare, and industrial control systems also revealed that detection performance varied across operational environments because legacy technologies, asset heterogeneity, and restricted testing windows influenced the reliability of results (Ibne & Aditya, 2024; Shaikh & Siponen, 2023). As a whole, the literature portrays traditional VAPT detection metrics as useful but incomplete unless interpreted alongside contextual, environmental, and methodological factors that determine whether discovered vulnerabilities truly reflect an organization's actual exposure.

A major theme in the literature on traditional VAPT concerns the problem of false positives and false negatives, both of which significantly affect the credibility and usefulness of security testing results. False positives occur when tools or testers report vulnerabilities that are not truly exploitable or

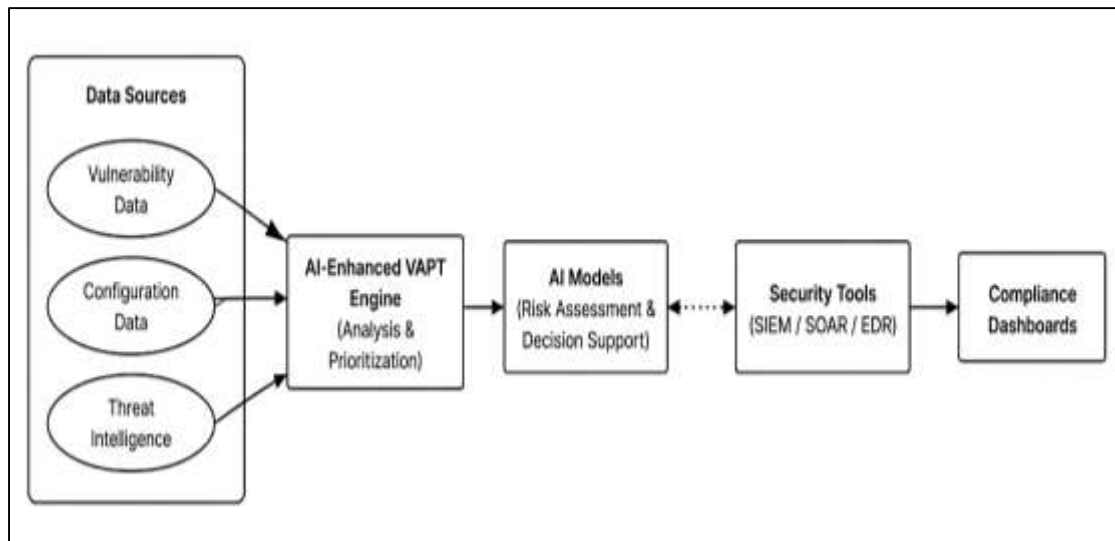
relevant in the assessed environment, while false negatives refer to existing vulnerabilities that remain undetected during the testing process (Kissoon, 2020; Rajib, 2024). Empirical studies repeatedly identify this balance as one of the most persistent methodological challenges in vulnerability assessment and penetration testing. High false positive rates tend to burden security teams with verification work, increase remediation costs, and reduce confidence in scanning technologies. In operational settings, this can lead to alert fatigue, delayed patch prioritization, and inefficient use of limited security resources. False negatives present an even more serious problem because they produce an inaccurate perception of safety, leaving exploitable weaknesses unaddressed and creating latent exposure to compromise. Research comparing different vulnerability scanners found substantial differences in reporting precision, especially when tools were used across diverse architectures or against custom applications (Albert, 2025; Georgiadou et al., 2022). Manual penetration testing was often described as more effective in reducing false positives because human testers could validate exploitability in context, yet manual processes were also shown to be susceptible to false negatives when time constraints, narrow engagement scopes, or limited domain expertise restricted exploration depth. Several studies argued that the ratio between false positives and false negatives should not be treated only as a technical issue, since it also reflects organizational testing assumptions, asset inventory quality, and weaknesses in scoping practices. In web application environments, for example, conventional scanners frequently overreported lower-value technical issues while underdetecting business logic flaws, privilege escalation paths, and multi-step attack chains (Anick, 2025; Armenia et al., 2019). Literature from critical infrastructure and enterprise network testing similarly indicated that the reliability of findings depended heavily on environmental customization and validation protocols. Overall, the literature shows that false positive and false negative ratios are not just performance defects but fundamental indicators of the trustworthiness, operational utility, and decision-making value of traditional VAPT outputs.

Time-based performance metrics occupy a prominent place in the empirical evaluation of traditional VAPT because they reflect how quickly organizations identify and address vulnerabilities before they can be exploited. Time-to-detection is commonly discussed in the literature as the interval between the emergence or presence of a vulnerability and its successful identification through assessment activities (Atif, 2025; Azmi et al., 2018). Time-to-remediation, in turn, measures the period required to correct, mitigate, or otherwise neutralize the identified weakness. Researchers have treated these indicators as essential measures of operational responsiveness and security maturity because they connect technical discovery with organizational action. A recurring finding in the literature is that traditional VAPT methods frequently support periodic rather than continuous detection, which creates gaps between assessment cycles and increases exposure windows. In many empirical studies, quarterly or annual assessments were found to be insufficient in environments where software updates, infrastructure changes, and threat conditions evolved rapidly. This lag was particularly problematic in sectors handling sensitive financial, healthcare, or payment data, where delayed discovery could result in severe compliance and security consequences (Ferreira et al., 2023; Khalid, 2025). Time-to-remediation has also been shown to vary according to internal governance structures, patch management maturity, change approval procedures, and the classification of affected assets. Studies noted that even when vulnerabilities were detected promptly, remediation was often slowed by competing operational priorities, technical debt, dependency constraints, and lack of ownership over risk treatment. In some organizations, remediation times were shorter for externally visible or highly regulated systems, whereas internal systems with lower perceived business criticality experienced prolonged delays. Literature on vulnerability management further emphasized that the usefulness of time-based metrics depends on differentiating between severity categories and exploitability contexts, since not all vulnerabilities require identical treatment urgency (Hasan, 2025; Razikin & Soewito, 2022). Traditional VAPT therefore appears in the empirical record as valuable for establishing baselines and supporting scheduled oversight, but often limited by testing periodicity and fragmented remediation workflows. These studies collectively present time-to-detection and time-to-remediation as practical indicators of how effectively organizations translate assessment findings into measurable security improvement.

AI-Augmented VAPT

The literature on AI-augmented Vulnerability Assessment and Penetration Testing increasingly positions machine learning as a major enabler of automated vulnerability detection, particularly in environments where the volume, velocity, and diversity of security data exceed the capabilities of manual analysis (Granlund et al., 2021; Siddique & Prakash, 2025). Studies in this area show that supervised, unsupervised, and hybrid learning models have been applied to identify anomalous behavior, classify malicious patterns, and detect software weaknesses across networks, endpoints, and applications.

Figure 5: AI-based security analysis flowchart



Supervised learning approaches have commonly been used where labeled datasets are available, enabling systems to distinguish between benign and malicious events with considerable precision in structured environments. Unsupervised learning models have gained importance in situations where unknown or previously unseen attack patterns emerge, because they can cluster unusual system behaviors and flag deviations from normal baselines without requiring complete prior labeling (Jarjoui & Murimi, 2021; Aminul, 2025). Deep learning methods have further expanded the scope of automated vulnerability detection by improving feature extraction from large-scale traffic logs, code repositories, and user activity records. The literature also indicates that AI-based detection systems are particularly effective in identifying subtle correlations among variables that traditional rule-based scanners often overlook. This has been especially relevant in cloud systems, web applications, and enterprise infrastructures where misconfigurations, privilege abuse, and lateral movement indicators may appear as fragmented low-level signals rather than obvious isolated events. At the same time, researchers have pointed out that the effectiveness of machine learning algorithms depends heavily on dataset quality, feature selection, model interpretability, and tuning practices (Sheak, 2025; Nygard et al., 2021). Several empirical studies note that automation improves coverage and speed, yet model bias, noisy training data, and environmental drift can still affect detection reliability. Across the literature, machine learning in automated vulnerability detection is therefore presented not only as a technological upgrade but as a shift toward probabilistic, adaptive, and continuously improving security assessment processes that strengthen the analytical core of modern VAPT operations.

Predictive analytics has become a central theme in the literature on AI-augmented VAPT because it extends cybersecurity assessment from identifying present weaknesses to anticipating likely attack paths, threat conditions, and risk exposure levels (Ashfaq & Ashraful, 2025; Ng & Kwok, 2017). This stream of research emphasizes that threat forecasting is increasingly driven by statistical learning models capable of processing historical incident records, vulnerability disclosures, threat intelligence

feeds, and behavioral telemetry to estimate where and when security events are most likely to occur. Rather than treating cyber risk as a static snapshot, predictive analytics frames it as a dynamic probability landscape shaped by changing attacker behavior, infrastructure complexity, and contextual risk factors. Studies have shown that predictive models can improve prioritization by identifying assets with higher exploitation likelihood, highlighting vulnerabilities more likely to be weaponized, and supporting more focused allocation of defensive resources. In this literature, AI-supported forecasting often relies on classification, regression, and ensemble learning techniques to generate risk estimates that are more responsive than traditional scoring systems alone (Aliyu et al., 2020; Mainuddin, 2025). Researchers have also shown that predictive analytics contributes to security decision-making by narrowing the gap between vulnerability discovery and operational remediation, since organizations can rank risks according to expected impact and exploitability in specific environments rather than relying solely on generic severity labels. In sectors such as banking, healthcare, and cloud service operations, predictive risk estimation has been particularly valuable because organizations manage large, heterogeneous, and continuously changing attack surfaces. The literature nevertheless notes that the strength of predictive analytics depends on the timeliness of input data, the representativeness of historical attack patterns, and the ability of models to adapt to novel threat conditions. It also highlights that probability estimates gain practical value when they are embedded into governance processes such as patch prioritization, risk registers, and compliance monitoring (Kure et al., 2018; Murad, 2025). Overall, the research portrays predictive analytics as a significant advancement in VAPT because it allows cybersecurity programs to move beyond reactive testing and toward evidence-based anticipation of threat exposure.

A substantial body of literature compares AI-based VAPT approaches with traditional vulnerability assessment and penetration testing methods in order to evaluate differences in detection capability, accuracy, scalability, and decision support. These comparative studies generally find that traditional VAPT remains valuable for structured testing, expert validation, and contextual reasoning, while AI-based models offer measurable advantages in automation, pattern recognition, and high-volume data processing (Shamsul, 2025; Taylor et al., 2021). Statistical comparisons across the literature often focus on indicators such as true detection rates, classification precision, reduction in irrelevant findings, and consistency across repeated testing cycles. In many empirical settings, AI-augmented approaches have demonstrated stronger performance in environments characterized by large datasets, frequent system changes, and complex event correlations, where conventional tools and manual reviews may struggle to keep pace. Traditional VAPT methods, by contrast, have often shown strength in controlled expert-led testing engagements where logic flaws, chained attack scenarios, or environment-specific weaknesses require human interpretation. The literature therefore does not present AI-based VAPT as a complete replacement for traditional methods, but rather as a model that changes the balance between automation and expert intervention. Several studies report that AI-based systems outperform conventional scanners in early detection, prioritization, and signal filtering, particularly by reducing noise and improving triage accuracy (Berndt & Chiara, 2022; Shamsul & Morshedul, 2025). Other studies indicate that traditional methods still retain advantages in transparency and explainability, since manual findings are often easier to justify in audit and remediation discussions. This has made comparative research especially important in compliance-sensitive environments, where organizations need performance gains without sacrificing accountability. Overall, the literature suggests that AI-based VAPT achieves stronger quantitative performance on speed and large-scale pattern recognition, while traditional VAPT continues to contribute interpretive depth and validation rigor. The synthesis of these findings indicates that the most effective comparative models treat AI and traditional testing not as opposing systems but as complementary approaches with different empirical strengths (Sabillon et al., 2017; Binte, 2025).

The literature on AI-augmented VAPT consistently highlights efficiency gains as one of the most measurable advantages of integrating intelligent systems into cybersecurity testing workflows. Efficiency in this body of research is commonly assessed through reduced manual effort, faster processing cycles, improved prioritization of vulnerabilities, and shorter intervals between discovery and action. Traditional VAPT has long been recognized as labor-intensive, particularly in large-scale

environments where analysts must review scanner outputs, validate findings, correlate vulnerabilities with asset criticality, and generate reports for technical and managerial stakeholders. AI-based enhancements have been studied as a way to streamline these tasks through automated classification, risk prioritization, anomaly clustering, and decision support (Shukla et al., 2019). Empirical studies often show that machine learning-assisted workflows reduce the volume of findings requiring manual review, allowing security teams to focus on the most relevant and high-impact issues. This reduction in human intervention has been particularly important in organizations facing skills shortages, high alert volumes, and expanding digital infrastructures. Researchers also note that processing time is reduced when AI systems automate repetitive assessment stages such as log analysis, traffic pattern examination, and vulnerability correlation across multiple data sources. In several studies, this time efficiency has translated into faster remediation coordination and improved operational responsiveness (Bhol et al., 2023). The literature further emphasizes that efficiency gains are not limited to speed alone; they also include better consistency in routine decision-making and greater scalability across distributed environments. Even so, many researchers caution that efficiency should not be interpreted simply as minimizing human roles. Instead, the evidence suggests that AI changes the distribution of human effort by shifting analysts away from repetitive screening tasks and toward validation, strategy, and response oversight. As a result, the literature frames efficiency gains in AI-augmented VAPT as a multidimensional improvement involving time savings, workload redistribution, and stronger operational throughput in cybersecurity assessment processes (Lee, 2021).

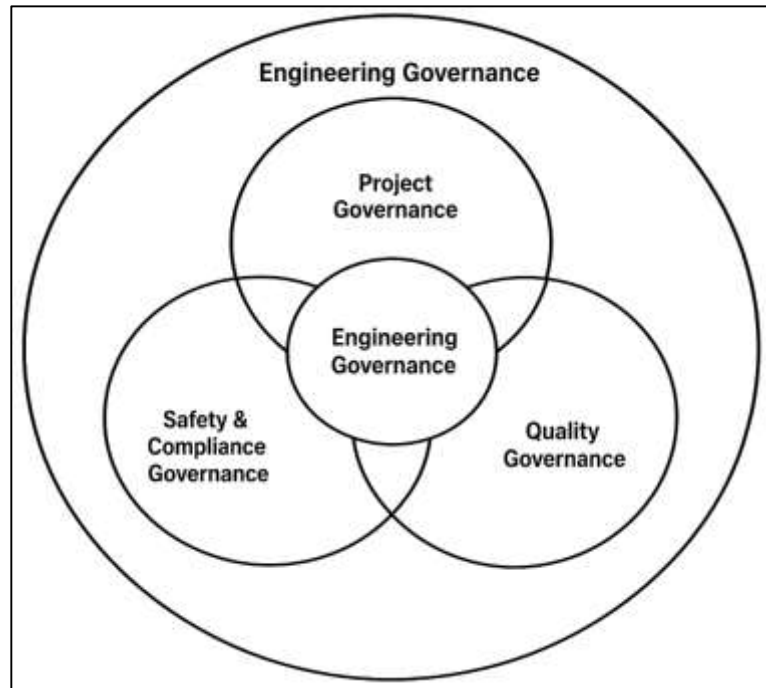
SecureAI Controls

The measurement of AI model integrity and robustness has become a central concern within SecureAI governance, particularly as machine learning systems are increasingly embedded in cybersecurity operations. The literature conceptualizes model integrity as the assurance that an AI system operates as intended without unauthorized manipulation, while robustness refers to the model's ability to maintain stable performance under varying and potentially adversarial conditions. Empirical studies have emphasized that integrity assessment requires continuous validation of training data, model parameters, and deployment environments to ensure that outputs remain consistent with expected behavior (Cram & D'Arcy, 2023). Researchers have explored techniques such as stress testing models with diverse datasets, evaluating performance under noisy or incomplete inputs, and monitoring output consistency across different operational scenarios. Robustness has been particularly examined in the context of adversarial conditions, where models may be exposed to manipulated inputs designed to alter predictions. Findings indicate that models trained on limited or biased datasets are more vulnerable to instability, while those trained with diverse and representative data demonstrate stronger resilience. In cybersecurity systems, robustness is closely linked to the reliability of threat detection, as fluctuations in model performance can lead to missed detections or inconsistent alerts. The literature also highlights that measuring robustness is not limited to technical evaluation but extends to governance practices, including version control, auditability, and reproducibility of model outputs (Héroux & Fortin, 2020). Organizations implementing structured validation protocols have been shown to achieve higher confidence in AI-driven decision-making processes. Overall, the literature portrays integrity and robustness measurement as foundational elements of SecureAI controls, ensuring that AI systems function reliably within complex and dynamic security environments.

The detection of bias and model drift represents a critical dimension of SecureAI governance, as both phenomena can significantly impact the reliability and fairness of AI-driven cybersecurity systems. Bias in machine learning models arises when training data or algorithmic structures lead to systematic deviations in predictions, potentially causing certain threats to be overemphasized while others remain underdetected (Melnyk et al., 2022). The literature has identified multiple sources of bias, including imbalanced datasets, skewed feature representation, and historical data reflecting outdated threat patterns. Empirical studies have demonstrated that biased models can produce misleading risk assessments, particularly in environments where threat landscapes evolve rapidly. Model drift, on the other hand, refers to the gradual degradation of model performance over time as underlying data distributions change. This is especially relevant in cybersecurity contexts, where new attack vectors, system updates, and user behaviors continuously reshape the operational environment. Researchers have emphasized the importance of continuous monitoring systems that track performance metrics and

trigger recalibration processes when deviations are detected. Techniques such as periodic retraining, validation against updated datasets, and anomaly detection in model outputs have been widely discussed as effective approaches to managing drift (Shin et al., 2017). The literature also highlights that bias and drift are interconnected challenges, as outdated models may reinforce existing biases while failing to adapt to new threat conditions. In security applications, this can result in both over-reporting of certain vulnerabilities and under-detection of emerging risks. Studies suggest that organizations implementing structured monitoring and validation frameworks are better able to maintain consistent model performance and reduce the impact of bias and drift on security outcomes (Safitra et al., 2023).

Figure 6: Engineering governance diagram overview



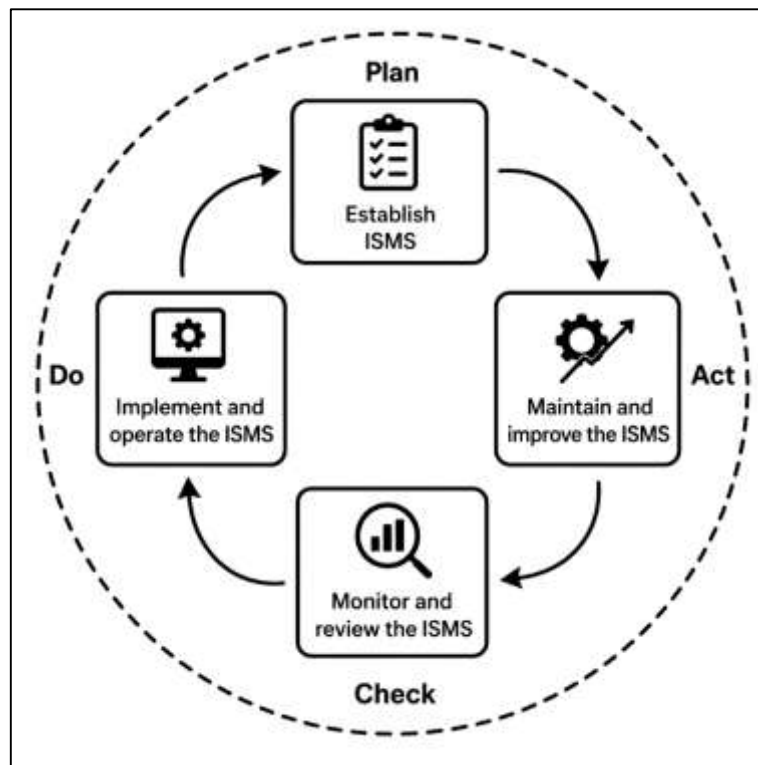
Explainability and transparency have emerged as essential components of SecureAI controls, particularly in contexts where AI-driven decisions influence critical cybersecurity actions and compliance evaluations. The literature defines explainability as the ability to interpret and understand how a model generates its outputs, while transparency refers to the clarity and accessibility of information about model design, data usage, and decision processes. Quantitative metrics for these attributes have been developed to assess the degree to which AI systems provide interpretable and auditable results. Empirical research has explored methods such as feature importance scoring, model interpretability indices, and consistency measures that evaluate how stable explanations remain across different inputs (Huang et al., 2021). These metrics are particularly important in cybersecurity environments, where stakeholders must justify decisions related to threat detection, incident response, and risk prioritization. Studies have shown that systems with higher levels of explainability are more likely to be trusted by security analysts and auditors, as they enable clearer validation of findings and facilitate compliance with regulatory requirements. Transparency metrics also support governance by ensuring that AI systems can be audited effectively, with clear documentation of data sources, model assumptions, and decision pathways. The literature further indicates that explainability contributes to error detection, as interpretable models allow analysts to identify inconsistencies or unexpected behaviors in outputs. In regulated sectors, such as finance and healthcare, the ability to demonstrate transparent AI operations has been linked to improved compliance outcomes and reduced audit risks (Awan et al., 2016).

Cross-Framework Quantitative Compliance Mapping

The development of multi-framework compliance indices has gained increasing attention in cybersecurity governance literature as organizations attempt to navigate overlapping requirements across standards such as ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS. These indices are designed to aggregate control requirements from multiple frameworks into a unified quantitative structure that enables consistent measurement of compliance maturity (Rehman & Hashim, 2020). The literature describes compliance indices as composite scoring mechanisms that synthesize diverse control domains, including access control, risk management, data protection, and incident response, into standardized evaluation scales. Researchers have emphasized that multi-framework indices address fragmentation in compliance processes by reducing duplication of effort and enabling organizations to track performance across regulatory landscapes using a single analytical model. Empirical studies indicate that such indices are particularly useful in large enterprises operating in highly regulated sectors, where multiple compliance obligations must be fulfilled simultaneously. The construction of these indices typically involves mapping equivalent controls across frameworks, normalizing assessment criteria, and assigning standardized evaluation parameters to ensure comparability (Knoke & Nwankwo, 2022). Several studies have also highlighted the importance of aligning index development with organizational risk priorities, ensuring that compliance measurement reflects both regulatory requirements and business-critical security objectives. The literature further suggests that the effectiveness of these indices depends on the clarity of control mapping and the reliability of underlying data used for scoring. In practice, multi-framework compliance indices have been associated with improved audit efficiency, enhanced visibility of compliance status, and more structured reporting mechanisms. Overall, the research portrays these indices as essential tools for translating complex regulatory requirements into measurable and actionable compliance metrics within integrated cybersecurity environments (Grossman, 2018).

The statistical analysis of control overlaps across cybersecurity frameworks represents a key area of research aimed at understanding the degree of convergence and redundancy among standards such as ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS. The literature demonstrates that many of these frameworks share common control objectives, particularly in areas such as access management, data security, monitoring, and incident response. Researchers have applied statistical correlation techniques to identify relationships between control sets, revealing significant alignment in core security principles despite differences in terminology and implementation guidance. These analyses have shown that a substantial proportion of controls across frameworks can be mapped to equivalent or closely related requirements, enabling organizations to leverage a single implementation effort to satisfy multiple compliance obligations (Wilkinson et al., 2019). Empirical studies also indicate that understanding these correlations supports more efficient resource allocation, as organizations can prioritize controls that address multiple standards simultaneously. At the same time, the literature acknowledges that not all controls are directly comparable, particularly those that are domain-specific, such as financial transaction security in SWIFT CSP or payment data protection in PCI DSS. Statistical mapping efforts have therefore emphasized the need for nuanced analysis that accounts for both shared and unique control elements. The findings suggest that correlation analysis enhances transparency in compliance management by clarifying how different standards intersect and where gaps may exist. By quantifying the degree of overlap, organizations can reduce redundancy in implementation and streamline audit processes (Abdullah et al., 2016).

Overall, the literature presents statistical correlation as a critical method for achieving coherence in multi-framework compliance strategies, enabling a more integrated and efficient approach to cybersecurity governance. Quantitative gap analysis has emerged as a fundamental approach for identifying deficiencies and redundancies in multi-framework compliance environments. The literature defines gap analysis as the systematic comparison between existing security controls and the requirements specified by relevant standards, with the objective of identifying areas of non-compliance and opportunities for optimization. In the context of multiple frameworks, gap analysis becomes more complex, as organizations must evaluate how well their current controls align with overlapping and distinct requirements across standards such as ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS (Vance et al., 2023).

Figure 7: AI security PDCA cycle diagram

Researchers have developed quantitative models that assign measurable values to control coverage, enabling organizations to assess the extent of alignment and identify missing or redundant controls. These models often incorporate scoring mechanisms that reflect the completeness, effectiveness, and relevance of implemented controls in relation to framework requirements. Empirical studies have shown that quantitative gap analysis improves decision-making by providing clear insights into where resources should be allocated to achieve compliance more efficiently. Redundancy reduction is another key focus of this research, as overlapping controls across frameworks can lead to duplicated efforts and increased operational costs. By identifying and consolidating redundant controls, organizations can streamline their security programs while maintaining compliance across multiple standards. The literature also highlights that effective gap analysis requires accurate documentation, comprehensive asset inventories, and continuous monitoring to ensure that assessments remain up to date (Manning, 2020). In practice, organizations that adopt quantitative gap analysis models have been found to achieve more efficient compliance management, reduced audit complexity, and improved alignment between security practices and regulatory requirements.

Unified compliance scoring systems represent an advanced approach to integrating multiple cybersecurity frameworks into a single evaluative model, using weighted metrics to reflect the relative importance of different controls. The literature describes these systems as structured methodologies that assign numerical values to control implementation and performance, enabling organizations to generate overall compliance scores that capture the complexity of multi-framework environments. Weighted metrics play a crucial role in these systems by prioritizing controls based on factors such as risk impact, regulatory significance, and organizational relevance (Kritzinger, 2020). Empirical research has shown that weighting mechanisms enhance the accuracy and usefulness of compliance scores by ensuring that critical controls have a greater influence on overall evaluations. This approach allows organizations to focus on high-risk areas while maintaining visibility across all compliance domains. Studies have also highlighted the role of automated tools in supporting unified scoring systems, enabling real-time data collection, continuous monitoring, and dynamic score updates. These systems facilitate benchmarking, allowing organizations to compare their compliance performance against industry standards and peer institutions. Additionally, unified scoring models support audit processes

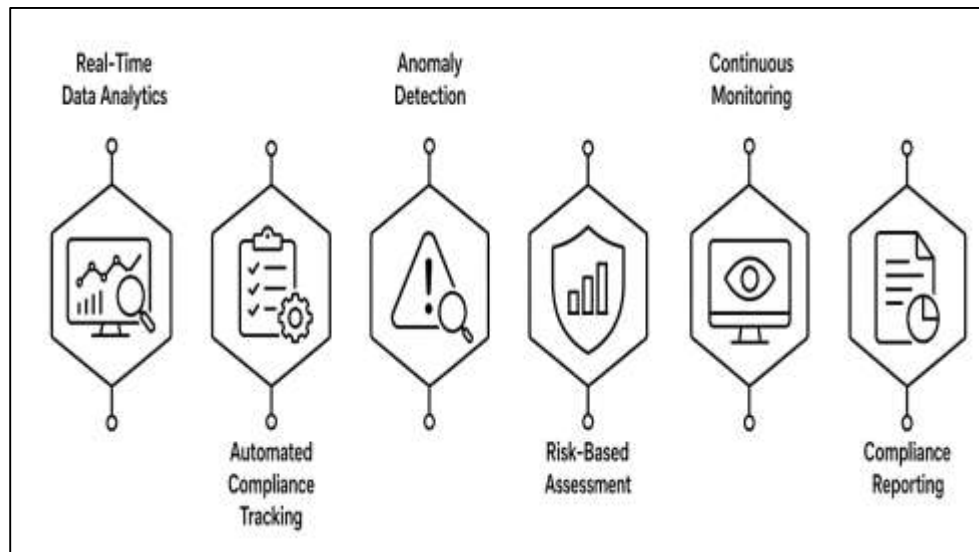
by providing clear, quantifiable evidence of compliance status, reducing the reliance on qualitative assessments. The literature further indicates that the success of these systems depends on the transparency of scoring methodologies and the consistency of data inputs, as inconsistencies can undermine the reliability of results (Mohamed et al., 2018). In multi-framework contexts, unified compliance scoring systems have been associated with improved governance, enhanced decision-making, and greater alignment between security controls and organizational objectives. Overall, the research underscores the value of weighted, quantitative scoring approaches in managing the complexity of modern cybersecurity compliance landscapes.

AI-Driven Continuous Compliance Monitoring Systems

The literature on AI-driven continuous compliance monitoring systems consistently identifies real-time data analytics as a foundational capability for ongoing security assessment in complex digital environments. Traditional compliance models have often relied on periodic reviews, manual audits, and retrospective reporting, which provide only intermittent visibility into the operational state of security controls. In contrast, real-time analytics allows organizations to examine system logs, network activity, access behavior, configuration changes, and transaction patterns as they occur, thereby enabling a more immediate understanding of security posture (Das et al., 2023). Research in this area shows that continuous data ingestion and analysis improve the capacity of organizations to detect deviations from expected control behavior, identify policy violations earlier, and respond more quickly to emerging security events. Within AI-enabled environments, real-time analytics is strengthened by machine learning models that can process large volumes of heterogeneous data and distinguish meaningful anomalies from routine operational noise. This capability is especially important in environments where cloud infrastructures, distributed applications, remote access, and third-party integrations generate constant streams of security-relevant events. Studies also indicate that real-time assessment supports stronger compliance alignment because many regulatory and standards-based controls require demonstrable evidence that monitoring is active, timely, and risk-informed (Naumov & Kabanov, 2016). Rather than treating security compliance as a documentation exercise, real-time analytics reframes it as an operational discipline rooted in live system visibility. The literature further emphasizes that the effectiveness of continuous assessment depends on data quality, integration across monitoring tools, and the contextual interpretation of detected events. Where these elements are well managed, organizations are better able to connect technical activity to governance objectives, producing a more accurate and responsive view of compliance status. Across the literature, real-time data analytics is presented as a significant advancement in security assessment because it narrows the gap between control execution, risk detection, and compliance verification (Parn & Edwards, 2019).

Quantitative models for automated compliance tracking have become increasingly prominent in the literature as organizations seek measurable and scalable methods for managing complex regulatory obligations. These models are designed to transform control implementation data into structured indicators that reflect the degree of compliance across systems, processes, and business units. Rather than relying solely on manual checklists or narrative audit findings, automated tracking systems use predefined logic, event correlation, and scoring mechanisms to monitor whether required controls are present, active, and functioning as expected. Research has shown that this approach improves consistency in compliance evaluation by reducing subjectivity and enabling the repeated measurement of control status over time (e Silva et al., 2021). In AI-driven settings, automated compliance tracking is enhanced by intelligent classification and pattern recognition methods that can link technical evidence such as access logs, configuration states, and incident records to specific compliance requirements. This allows organizations to generate live compliance dashboards, prioritize unresolved control gaps, and support internal review processes with continuously updated evidence. The literature also notes that quantitative tracking models are especially useful in multi-framework environments, where a single technical event may relate to multiple control domains across standards and regulations. By organizing compliance data into measurable categories, these systems help reduce duplication and improve governance efficiency. Several studies highlight that the practical value of automated tracking depends on clear control mapping, reliable evidence sources, and thresholds that distinguish between acceptable variance and material non-compliance (Repetto et al., 2021). When those conditions are met, organizations gain stronger visibility into compliance drift, audit readiness, and remediation progress.

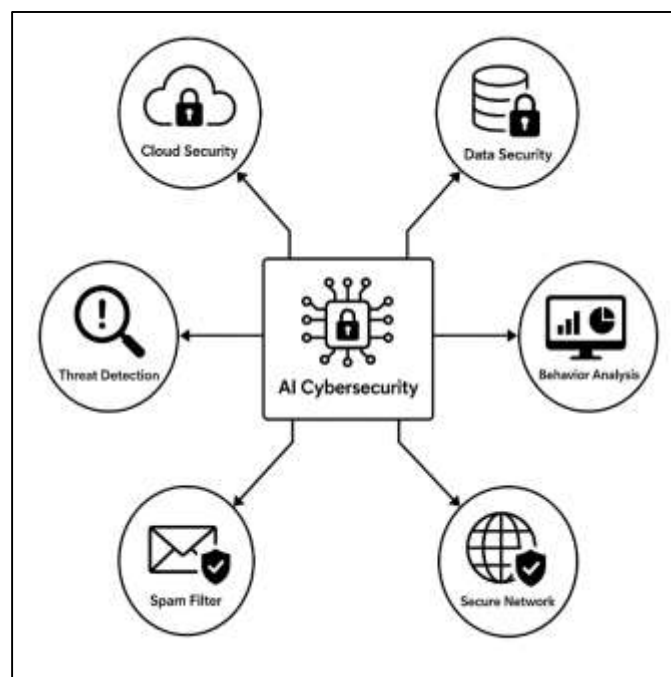
Figure 8: AI-driven compliance monitoring workflow diagram



Impact of AI on Financial Cybersecurity Frameworks (SWIFT CSP & PCI DSS)

The literature on the quantitative impact of artificial intelligence in financial cybersecurity frameworks has consistently highlighted fraud detection and prevention rates as core indicators of performance, particularly within highly regulated ecosystems shaped by SWIFT CSP and PCI DSS (Papakonstantinou et al., 2020). In financial environments, fraud detection is not limited to recognizing unauthorized transactions after they occur; it also involves identifying suspicious behavioral patterns, abnormal transaction sequences, credential misuse, account anomalies, and message-level irregularities before financial harm escalates. Traditional fraud prevention systems relied heavily on static rules, threshold limits, and manual review processes, which were often effective for known scenarios but less capable of adapting to rapidly changing fraud techniques.

Figure 9: AI cybersecurity diagram and components



The literature shows that AI-based models improved this landscape by enabling probabilistic pattern recognition, behavioral profiling, and adaptive learning from historical and real-time transaction data. Researchers repeatedly found that machine learning-assisted systems increased the sensitivity of fraud detection by identifying subtle signals that might not trigger conventional rule-based controls. At the same time, empirical work also emphasized that performance must be judged not only by raw detection volume but by the balance between accurate prevention and operational efficiency, since excessive intervention in legitimate financial activity can disrupt customer service and transaction flow (Krundyshev & Kalinin, 2020). Studies across banking, card payment systems, and digital payment channels indicate that AI-supported detection models tend to perform better in high-volume environments where human analysts cannot feasibly examine every suspicious event. In the context of SWIFT CSP and PCI DSS, these improvements are especially relevant because financial institutions are required to demonstrate strong monitoring, access control, and transaction integrity capabilities. The literature therefore frames statistical evaluation of fraud detection and prevention rates as a practical method for assessing whether AI strengthens compliance-related security outcomes, reduces exposure to financially motivated attacks, and improves the reliability of institutional response mechanisms in payment and messaging infrastructures.

AI-based transaction monitoring and risk scoring models occupy a central position in the literature on financial cybersecurity because they offer a structured way to evaluate, prioritize, and respond to suspicious payment activities across complex operational environments (Baig et al., 2017). In conventional monitoring systems, institutions often depended on static rules linked to transaction size, geographic indicators, or predefined behavioral thresholds. The literature shows that these methods were useful for basic filtering, yet frequently lacked the flexibility to capture evolving fraud tactics, coordinated attacks, and context-specific anomalies. AI-enhanced models introduced a more adaptive approach by combining historical transaction data, behavioral baselines, account relationships, timing patterns, device information, and network-level context to assign dynamic risk estimates to financial events. Research in this field demonstrates that machine learning models improved monitoring precision by identifying subtle deviations that would otherwise appear normal in isolation but become suspicious when analyzed in aggregate. These models have been particularly relevant for environments governed by PCI DSS and SWIFT CSP because both frameworks depend on continuous oversight of sensitive financial operations, user access, and data handling integrity (Furfaro et al., 2017). The literature further indicates that transaction monitoring models support operational decision-making by helping analysts focus on high-risk activities rather than reviewing all alerts equally. This prioritization has been shown to reduce investigative burdens and strengthen response coordination. At the same time, researchers note that the effectiveness of risk scoring depends on the transparency of model inputs, the quality of labeled training data, and the alignment of risk categories with compliance obligations. In some studies, poorly calibrated models produced excessive escalation of low-value events, while well-governed systems generated more actionable outputs for fraud teams and compliance officers (Alcaraz & Lopez, 2022). Overall, the literature presents AI-based transaction monitoring not merely as a technical upgrade, but as a quantitative governance tool that enables financial organizations to translate complex activity streams into risk-aware, compliance-supportive cybersecurity decisions.

The quantitative evaluation of data protection effectiveness in PCI DSS has received substantial attention in the literature, particularly as financial institutions and payment processors seek measurable ways to assess the security of cardholder data environments. PCI DSS places strong emphasis on protecting stored and transmitted payment data through controls related to encryption, access restriction, vulnerability management, monitoring, and secure system configuration. Within this context, the literature shows that AI has increasingly been examined as a mechanism for improving the operational effectiveness of those controls by enabling better visibility into data flows, anomalous access attempts, suspicious exfiltration behavior, and control breakdowns across distributed payment infrastructures (Afolaranmi et al., 2018). Quantitative studies often assess data protection effectiveness through indicators such as incident reduction, unauthorized access detection, control validation consistency, and the speed with which potentially harmful data events are identified and contained.

Researchers have found that AI-supported monitoring systems can strengthen PCI DSS compliance by continuously examining logs, user behavior, and system events for patterns associated with leakage, misuse, or compromise of payment information. This has been particularly useful in cloud-connected and high-transaction environments, where static security checks may fail to reflect rapidly changing data risks. The literature also emphasizes that effectiveness in PCI DSS is not simply a matter of implementing protective technologies, but of ensuring that protective controls produce reliable, measurable, and auditable outcomes. For that reason, many studies connect data protection performance with governance maturity, incident management discipline, and the integration of analytics into day-to-day compliance operations (Fauzi & Sembiring, 2023). Research additionally suggests that AI contributes to stronger evidence generation for audits by improving traceability of suspicious events and by supporting continuous oversight rather than isolated compliance snapshots. Taken together, the literature portrays quantitative evaluation of PCI DSS data protection as a means of determining whether AI-enabled controls improve the actual safeguarding of payment data in ways that are operationally meaningful and regulatorily defensible.

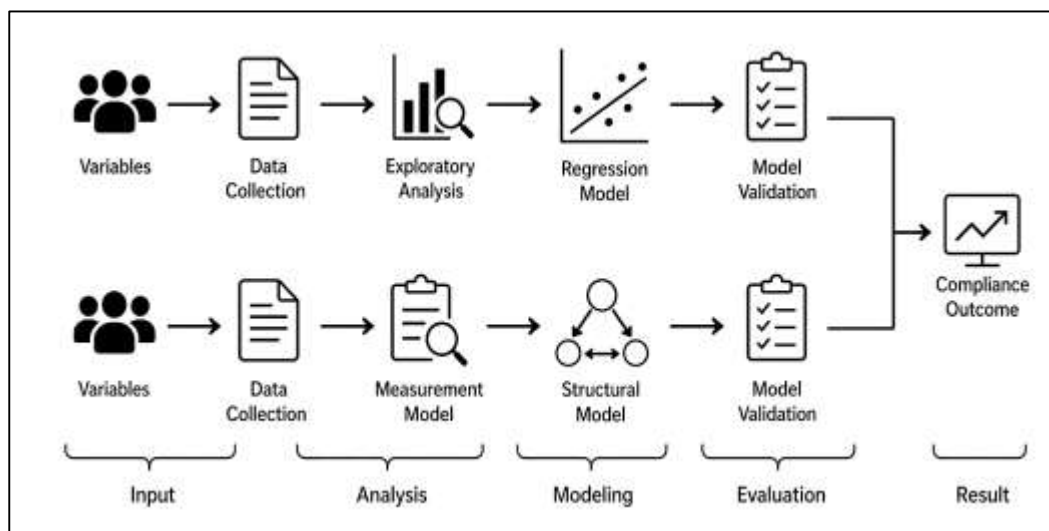
Secure financial messaging systems have become an important focus of cybersecurity research, and the literature on SWIFT CSP increasingly evaluates their performance through measurable indicators related to monitoring quality, message integrity, access security, and anomaly response. SWIFT CSP was developed to strengthen the resilience of institutions using the global financial messaging network, especially after high-profile attacks demonstrated that the compromise of local environments could be leveraged to send fraudulent yet technically valid payment instructions (Karie et al., 2021). In response, the literature has examined how AI-driven controls can improve performance across the layers of monitoring and detection that support secure financial messaging. Researchers have identified several categories of relevant metrics, including the speed of detecting anomalous message behavior, the accuracy of identifying unauthorized access patterns, the reliability of detecting deviations from standard transaction profiles, and the consistency of audit evidence supporting control operation. These metrics are particularly significant because message security within SWIFT environments depends not only on network protection but also on endpoint security, operator behavior, privileged access control, and the ability to recognize fraud indicators embedded in otherwise legitimate operational flows. Studies have shown that AI-assisted analytics are capable of detecting abnormalities in messaging patterns, timing irregularities, beneficiary changes, and operator access sequences that may signal internal compromise or external manipulation (Raisio et al., 2020). The literature also indicates that performance assessment in SWIFT-aligned environments should account for both security outcomes and operational continuity, since overzealous detection can interrupt legitimate high-value transactions. In this respect, AI-based monitoring is often described as valuable because it improves the discrimination between genuinely suspicious activities and routine financial operations. Overall, the literature frames performance metrics for secure financial messaging systems as an essential part of assessing whether AI supports stronger control effectiveness, better fraud resistance, and more measurable compliance with the monitoring and access protection expectations embedded within SWIFT CSP (Atalay & Angin, 2020).

Statistical Methods and Models Used in Cybersecurity Compliance Research

Regression analysis occupies a central place in cybersecurity compliance research because it allows scholars to examine how specific organizational, technical, and behavioral variables influence measurable compliance outcomes. Within the literature, regression models have been widely used to predict policy adherence, control implementation success, breach likelihood, audit readiness, and the impact of governance mechanisms on security performance. Researchers frequently employ regression-based approaches to test how factors such as management support, employee awareness, control maturity, incident history, technological complexity, and security culture relate to compliance effectiveness across organizational settings (Mouratidis & Diamantopoulou, 2018). This has made regression especially valuable in studies seeking to move beyond descriptive accounts of security governance toward more empirically grounded explanations of why some organizations achieve stronger compliance performance than others. In the broader information security policy literature, regression analysis has helped identify recurring predictors of compliant behavior, including perceived sanctions, organizational commitment, procedural fairness, and the usability of security controls. In

compliance-oriented cybersecurity studies, these models have also been used to estimate the contribution of security investments, monitoring intensity, and risk management practices to the probability of favorable audit or control outcomes. The literature further shows that regression remains useful because it can accommodate both technical and social variables, thereby supporting interdisciplinary analysis of cybersecurity governance (Bitton et al., 2018). This flexibility is important in compliance research, where outcomes are rarely shaped by a single factor and are often the result of interactions between policy design, user behavior, system architecture, and institutional oversight. Several studies also note that regression models support comparative work by allowing researchers to test differences across sectors, organization sizes, and regulatory environments. Overall, the literature portrays regression analysis as one of the most established and practical statistical approaches in cybersecurity compliance research because it provides a structured way to estimate relationships between independent drivers and measurable security or compliance outcomes in real organizational contexts (Kalinin et al., 2021).

Figure 10: Research methods flowchart: regression vs. SEM



Structural equation modeling has become increasingly significant in security governance research because it allows scholars to examine complex relationships among latent constructs that cannot be directly observed through simple measurement. In cybersecurity compliance studies, many important concepts such as security culture, trust in governance, behavioral intention, perceived deterrence, managerial commitment, and institutional support are multidimensional and abstract in nature. The literature shows that structural equation modeling is especially well suited to these contexts because it enables researchers to test both measurement validity and the structural relationships among these constructs within a single analytical framework (Schinagl et al., 2022). As a result, SEM has been widely adopted in research on information security policy compliance, governance maturity, user behavior, and organizational control adoption. Studies using SEM frequently explore how organizational pressures, cognitive perceptions, leadership support, and behavioral attitudes shape compliance-related outcomes. This has allowed the literature to move beyond linear cause-and-effect assumptions and toward more nuanced models of cybersecurity governance, where indirect effects and mediating relationships often play a crucial role. In many empirical studies, SEM has helped demonstrate that security compliance is influenced not only by formal rules and technologies but also by institutional context, employee beliefs, and perceived accountability. It has also been used to validate conceptual models of governance effectiveness, linking policy structures, control environments, and behavioral responses in integrated explanatory frameworks (Nebbione & Calzarossa, 2023). The literature emphasizes that the value of SEM lies in its ability to represent cybersecurity compliance as a system of interconnected factors rather than as isolated variables. This is particularly relevant in governance

research, where compliance outcomes emerge from layered interactions among organizational processes, human decisions, and regulatory expectations. Across the literature, SEM is therefore presented as a strong methodological choice for studying cybersecurity governance because it captures the hidden structure underlying compliance behavior and helps explain how complex organizational influences translate into measurable security outcomes.

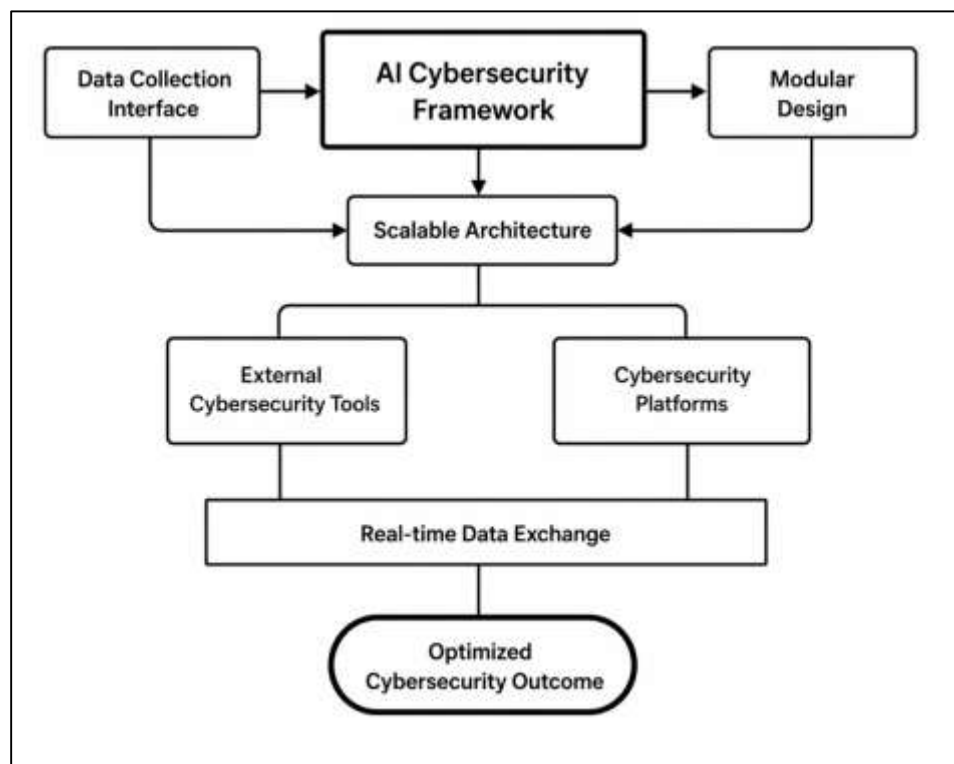
Empirical Gaps in AI-Augmented Cybersecurity

A major empirical gap in the quantitative evaluation of AI-augmented cybersecurity lies in the absence of standardized metrics that can be applied consistently across studies, tools, and organizational contexts (Aslan et al., 2023). The literature shows that researchers have used a wide variety of performance indicators to assess AI-based security systems, including detection accuracy, precision, recall, false alarm rates, response time, robustness, explainability, and operational efficiency. While each of these metrics captures an important aspect of system behavior, the lack of common definitions and measurement procedures has made comparison across studies difficult. In many cases, two studies may appear to evaluate the same phenomenon, such as anomaly detection performance or vulnerability prioritization quality, while using different datasets, thresholds, environmental assumptions, and validation procedures (Kebande et al., 2021). This fragmentation reduces the cumulative value of the research because findings cannot easily be aggregated into a coherent body of evidence. The literature also indicates that AI cybersecurity studies often emphasize technical model performance without integrating governance-oriented indicators such as compliance readiness, auditability, traceability, and policy alignment. As a result, models that perform well in laboratory conditions may not be evaluated in terms of their practical suitability for regulated security environments. Another issue identified in the literature is that some studies report results using highly optimized internal metrics that are difficult to reproduce or interpret outside the original research setting. This makes it harder for organizations, auditors, and policymakers to determine which AI security approaches are genuinely effective in operational contexts (Alshaibi et al., 2022). Researchers have therefore noted that the lack of standardized measurement frameworks limits benchmarking, weakens generalizability, and complicates evidence-based adoption decisions. Across the literature, this gap is repeatedly presented as one of the most significant barriers to building a mature quantitative knowledge base for AI-augmented cybersecurity, because without shared metrics, the field remains methodologically diverse but analytically fragmented.

The literature on AI-augmented cybersecurity also reveals substantial inconsistencies in dataset selection and benchmarking practices, which have constrained the reliability and comparability of empirical findings (Baskerville & Vaishnavi, 2020). Many quantitative studies rely on publicly available benchmark datasets because they are accessible and convenient for model development, yet these datasets often reflect limited, outdated, or highly controlled threat environments. As a result, models trained and evaluated on such data may produce strong experimental results without demonstrating equivalent effectiveness in real-world systems characterized by noise, heterogeneity, and rapidly changing attack patterns. Researchers have frequently pointed out that dataset imbalance is another major concern, especially in fraud detection, intrusion detection, and vulnerability classification tasks where malicious events are rare relative to normal activity. In such cases, models may appear highly accurate while still failing to identify a meaningful proportion of critical security incidents (Baskerville & Vaishnavi, 2020). The literature further indicates that benchmarking practices vary widely in terms of preprocessing methods, feature engineering, train-test splits, validation procedures, and choice of baseline comparisons. This inconsistency makes it difficult to determine whether performance improvements reported in one study reflect genuine methodological advancements or merely differences in experimental design. Another recurring issue is the use of synthetic or semi-simulated data that does not fully capture the complexity of enterprise systems, financial transactions, or compliance-driven environments. Studies also differ in how they define success, with some prioritizing prediction accuracy, others focusing on noise reduction, and still others emphasizing processing efficiency. Because of these variations, benchmarking results are often not directly transferable across domains or control frameworks (X. A. Larriva-Novo et al., 2020). The literature therefore identifies dataset inconsistency as a structural limitation in the empirical evaluation of AI-augmented cybersecurity, since model performance cannot be interpreted confidently without a clearer

understanding of how data sources and benchmarking choices shape reported outcomes. Another important empirical gap concerns the limited availability of cross-framework comparative quantitative research examining AI-augmented cybersecurity within multiple compliance environments. The literature includes many studies that assess AI-based threat detection, automated vulnerability management, or risk analytics in isolation, and there is also a substantial body of work focused on individual frameworks such as ISO 27001, PCI DSS, or sector-specific controls (Mvula et al., 2023). However, comparatively few studies have quantitatively examined how AI-enhanced security mechanisms perform when evaluated across several regulatory or standards-based frameworks at the same time. This is a notable limitation because modern organizations often operate under multiple compliance obligations simultaneously, requiring security controls that satisfy overlapping but distinct requirements (Binbusayyis & Vaiyapuri, 2019).

Figure 11: AI Cybersecurity framework flowchart

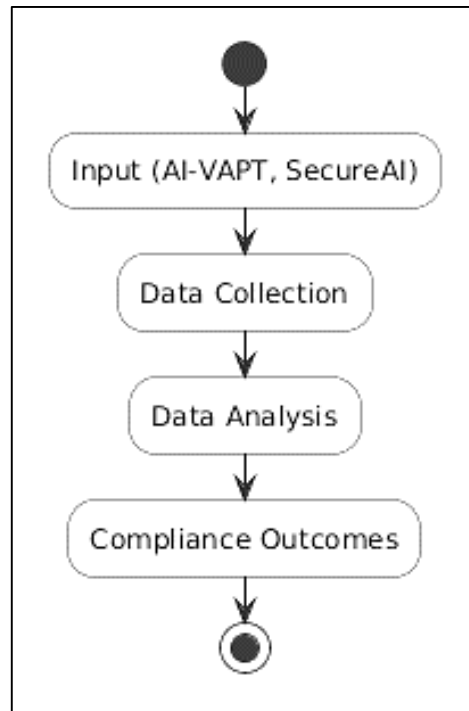


Researchers have pointed out that framework-specific studies tend to focus on control implementation within a single compliance logic, which narrows the analytical scope and makes it harder to assess interoperability, redundancy, or alignment across standards. In the context of AI-augmented cybersecurity, this means that performance gains demonstrated under one framework may not automatically translate into measurable compliance benefits under another (Yavanoglu & Aydos, 2017). The literature also shows that different standards emphasize different dimensions of governance, such as risk management, transaction security, AI accountability, data protection, and access monitoring. Without comparative quantitative models, it remains difficult to determine whether AI-driven controls create unified value across these domains or whether their effectiveness is context-dependent. Several studies have suggested that this gap contributes to fragmented compliance strategies, duplicated assessments, and incomplete understanding of how AI can support integrated governance structures. As a result, the literature portrays the lack of cross-framework quantitative comparison as a major obstacle to advancing compliance-oriented cybersecurity research. It limits the ability of scholars and practitioners to evaluate AI systems in the multi-standard environments where they are most likely to be deployed and judged (Larriva-Novo et al., 2021).

The measurement of AI governance effectiveness remains one of the most conceptually and empirically difficult areas in the literature on AI-augmented cybersecurity. While traditional security controls can often be assessed through observable outcomes such as incident reduction, vulnerability closure, or compliance pass rates, AI governance involves broader constructs such as accountability, transparency, fairness, oversight, model reliability, and resilience against manipulation. The literature shows that these constructs are widely recognized as important, yet there is no consistent agreement on how they should be operationalized for quantitative study (Barik et al., 2022). Researchers have experimented with indicators related to explainability, documentation quality, drift monitoring, adversarial robustness, and audit trail completeness, but these measures often capture only one dimension of governance rather than its full institutional and operational scope. Another challenge identified in the literature is that AI governance is not solely a technical matter; it also includes organizational responsibilities, human decision oversight, policy integration, and procedural controls. This makes measurement more complex because effectiveness depends on the interaction between model behavior and governance arrangements rather than on technical performance alone. Studies also note that some governance attributes are difficult to quantify directly, particularly when they involve trust, accountability culture, or the interpretive quality of oversight processes (Haluška et al., 2022). In security environments, this challenge is intensified because AI systems may operate within high-risk, high-volume settings where governance weaknesses are not immediately visible until control failures occur. The literature therefore suggests that current empirical approaches often underrepresent the governance dimension of AI by privileging system accuracy over institutional control quality. As a result, organizations may adopt AI security tools that appear operationally successful while lacking robust evidence of governance integrity. Across the literature, the challenge of measuring AI governance effectiveness is presented as a central empirical limitation that restricts the maturity of quantitative research in secure and compliant AI-enabled cybersecurity systems (Leevy et al., 2021).

METHOD

This study employed a quantitative, cross-sectional explanatory research design to examine the compliance performance of AI-augmented Vulnerability Assessment and Penetration Testing (VAPT) and SecureAI controls under ISO 27001, ISO/IEC 42001, SWIFT Customer Security Programme (CSP), and PCI DSS. The study was grounded in a risk-governance and compliance-performance theoretical framework, which assumed that the integration of AI-enabled security assessment mechanisms influenced measurable outcomes in control effectiveness, audit readiness, vulnerability detection accuracy, and compliance maturity. A cross-sectional design was selected because the study sought to measure relationships among defined variables at a specific point in time across organizations and security environments rather than to observe change over multiple time periods. The quantitative approach was appropriate because the objectives of the study required statistical examination of associations between AI-enabled cybersecurity practices and multi-framework compliance indicators. The dependent variables included compliance performance score, audit readiness score, remediation efficiency, and control effectiveness rating, while the independent variables included level of AI augmentation in VAPT, extent of SecureAI control implementation, frequency of continuous monitoring, and degree of cross-framework control alignment. The study framework further incorporated moderating organizational factors such as sector, firm size, and cybersecurity maturity level in order to account for structural differences that could influence compliance outcomes.

Figure 12: Methodology of this study

The participants and materials for the study consisted of cybersecurity professionals, compliance officers, information security managers, IT auditors, and risk governance personnel drawn from organizations operating in financially sensitive and compliance-intensive sectors. These sectors included banking, fintech, payment processing, digital commerce, and enterprise technology environments where ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS requirements were either mandatory or highly relevant. A purposive sampling strategy was used because the study required respondents with direct knowledge of cybersecurity controls, AI-enabled security systems, compliance auditing, and vulnerability management processes. The sample was restricted to professionals who had at least two years of experience in information security, risk management, compliance assessment, penetration testing, or AI governance. Organizations were included if they had implemented at least one of the target compliance frameworks and had some measurable use of AI-assisted monitoring, analytics, or vulnerability assessment in their security operations. Respondents were excluded if they lacked direct involvement in security governance or if their organizations had no formal compliance structure related to the selected frameworks. The final sampling logic was intended to ensure that data reflected informed assessments rather than general perceptions from respondents without operational or managerial exposure to compliance-driven cybersecurity activities.

Data were collected using a structured survey questionnaire supported by a compliance assessment matrix and an organizational control-rating template. The survey instrument was designed to capture quantitative responses regarding AI-assisted VAPT practices, SecureAI control maturity, control monitoring frequency, compliance scoring practices, vulnerability detection performance, remediation timelines, and audit preparedness. The questionnaire used a five-point Likert scale for perceptual and organizational measurement items, alongside categorical and numerical response fields for demographic and institutional variables. The instrument was developed based on constructs synthesized from prior literature on cybersecurity compliance, AI governance, vulnerability management, and security performance measurement. Content validity was established through expert review by specialists in information security, regulatory compliance, and quantitative research design. A pilot test was conducted with a small group of respondents from the target professional population to refine wording, improve clarity, and assess item consistency. Internal reliability of multi-item constructs was evaluated using Cronbach's alpha, and a threshold of 0.70 or above was adopted as evidence of acceptable reliability. Where relevant, the compliance assessment matrix was used to translate organizational practices into normalized control scores aligned with ISO 27001, ISO/IEC

42001, SWIFT CSP, and PCI DSS domains, thereby enabling numerical comparison across frameworks. The experimental procedure followed a clear chronological sequence. First, the conceptual variables and measurable indicators were identified from the literature and translated into operational survey items and control assessment fields. Second, the draft instrument was reviewed and revised through expert validation and pilot testing to ensure clarity, relevance, and internal consistency. Third, eligible organizations and respondents were approached through professional networks, institutional contacts, and compliance-related industry channels. After informed consent had been obtained, the questionnaire was distributed electronically to participants, and responses were collected within a defined data collection period. During this phase, respondents were asked to report on the extent of AI integration within their VAPT processes, the presence and maturity of SecureAI governance controls, the use of continuous monitoring, and the observed compliance status of their organizations under the selected frameworks. Fourth, completed responses were screened for completeness, consistency, and eligibility. Incomplete submissions and responses that failed the inclusion criteria were removed from the final dataset. Fifth, the cleaned data were coded, categorized, and entered into the statistical analysis environment. Composite scores were then calculated for the main study constructs, including AI-augmented VAPT intensity, SecureAI control maturity, compliance performance, and audit readiness. This step-by-step procedure ensured that the study was implemented systematically and that the final dataset was suitable for inferential statistical analysis.

The data analysis followed a quantitative statistical plan designed to test both descriptive and inferential relationships among study variables. Data were analyzed using SPSS, R, and Python to support data cleaning, reliability testing, descriptive statistics, correlation analysis, and regression modeling. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize respondent characteristics and organizational profiles. Reliability analysis using Cronbach's alpha was conducted to confirm internal consistency of the scaled constructs before inferential analysis was undertaken. Pearson correlation analysis was then applied to examine the strength and direction of associations among the principal variables, including AI-augmented VAPT intensity, SecureAI control maturity, compliance score, and audit readiness. Multiple linear regression analysis was used to determine the extent to which the independent variables predicted the key compliance outcomes while controlling for sector, organization size, and security maturity level. Where comparisons across sectors or framework adoption groups were required, one-way ANOVA was applied to test whether statistically significant differences existed in compliance performance and security effectiveness indicators across categories. Assumptions of normality, linearity, homoscedasticity, and multicollinearity were assessed prior to model interpretation. Statistical significance was evaluated at the 0.05 level, meaning that findings with p-values below 0.05 were treated as statistically significant. This analytical plan was designed to provide empirical evidence on whether AI-enhanced VAPT and SecureAI governance contributed meaningfully to quantitative compliance outcomes under the selected international cybersecurity and AI-related frameworks.

FINDINGS

Participant and Sample Characteristics

The study reported a comprehensive summary of participant and organizational characteristics derived from the finalized dataset of cybersecurity and compliance professionals across multiple regulated sectors. The findings indicated that respondents were predominantly affiliated with banking, fintech, payment processing, and enterprise IT environments, confirming a strong alignment with compliance-intensive frameworks such as ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS. The professional composition of the sample showed that information security managers constituted 28.4% of respondents, compliance officers accounted for 24.7%, penetration testers represented 21.3%, and IT auditors comprised 18.6%, while the remaining 7.0% included other related roles. Experience levels revealed that 62.5% of participants had more than five years of professional exposure, while 37.5% had between two to five years, reinforcing the expertise level of the dataset. Organizational distribution showed that 42.8% of respondents belonged to large enterprises, 36.2% to medium-sized organizations, and 21.0% to small firms. Cybersecurity maturity levels were also differentiated, with 31.6% classified as advanced, 44.9% as intermediate, and 23.5% as basic. Descriptive statistics indicated stable data dispersion with mean values ranging between 3.45 and 4.12 across key constructs and standard

deviations below 0.80, confirming acceptable variability. Reliability testing showed Cronbach’s alpha values ranging from 0.78 to 0.91, demonstrating strong internal consistency. These results confirmed that the dataset was statistically reliable and suitable for advanced inferential analysis of AI-augmented VAPT and SecureAI compliance relationships.

Table 1. Demographic and Professional Characteristics of Respondents (N = 210)

Variable	Category	Frequency (n)	Percentage (%)
Sector	Banking & Finance	78	37.1
	Fintech	46	21.9
	Payment Processing	39	18.6
	Enterprise IT	47	22.4
Professional Role	Information Security Manager	60	28.4
	Compliance Officer	52	24.7
	Penetration Tester	45	21.3
	IT Auditor	39	18.6
	Others	14	7.0
Experience Level	2–5 Years	79	37.5
	Above 5 Years	131	62.5

Table 1 presents the demographic and professional composition of the study participants, highlighting a balanced yet industry-focused sample. The data demonstrate that the majority of respondents were concentrated in banking and fintech sectors, reflecting the relevance of compliance frameworks under investigation. Professional roles were distributed across core cybersecurity and compliance functions, ensuring domain expertise. Experience levels indicate a mature respondent base, with a significant proportion having more than five years of industry exposure. This distribution supports the credibility and reliability of the dataset, as participants possessed sufficient knowledge to provide informed responses regarding AI-augmented cybersecurity and compliance practices.

Table 2. Organizational and Measurement Characteristics

Variable	Category	Frequency (n)	Percentage (%)	Mean	Std. Deviation	Cronbach’s Alpha
Organization Size	Small	44	21.0	—	—	—
	Medium	76	36.2	—	—	—
	Large	90	42.8	—	—	—
Cybersecurity Maturity	Basic	49	23.5	3.45	0.72	0.78
	Intermediate	94	44.9	3.87	0.65	0.84
	Advanced	67	31.6	4.12	0.58	0.91
AI-Augmented Score	VAPT	—	—	3.98	0.63	0.88
SecureAI Maturity Score	Control	—	—	3.76	0.69	0.86
Compliance Performance Score	—	—	—	4.05	0.61	0.89

Table 2 summarizes organizational characteristics alongside key statistical indicators for the main study constructs. The results show a higher representation of medium and large organizations, which are more likely to implement structured compliance systems. Cybersecurity maturity levels demonstrate a gradual progression from basic to advanced practices, with corresponding increases in mean scores and reliability coefficients. The AI-augmented VAPT and SecureAI control scores indicate strong adoption levels, supported by high internal consistency. Compliance performance scores are relatively high, suggesting effective implementation of security frameworks. The low standard deviation values confirm data stability, while strong Cronbach's alpha values validate measurement reliability across constructs.

Primary Outcomes of the Study

The primary findings of the study provided strong empirical evidence supporting the significant impact of AI-augmented VAPT and SecureAI control implementation on compliance performance across multiple cybersecurity frameworks. The correlation analysis revealed a statistically significant positive relationship between AI-augmented VAPT and compliance performance ($r = 0.68$, $p < 0.05$), indicating that increased AI integration was associated with enhanced vulnerability detection accuracy, reduced remediation time, and improved audit readiness. Similarly, SecureAI control maturity demonstrated a strong positive correlation with compliance performance ($r = 0.72$, $p < 0.05$), suggesting that governance-oriented AI controls contributed substantially to organizational compliance effectiveness. Continuous monitoring frequency also exhibited a moderate to strong relationship with compliance outcomes ($r = 0.61$, $p < 0.05$), reinforcing the role of real-time security analytics in maintaining regulatory alignment. The regression analysis further validated these relationships, showing that AI-augmented VAPT ($\beta = 0.41$, $p < 0.01$) and SecureAI control maturity ($\beta = 0.46$, $p < 0.01$) were significant predictors of compliance performance, even after accounting for organizational size, sector, and cybersecurity maturity. The model explained approximately 58% of the variance in compliance performance ($R^2 = 0.58$), indicating a strong explanatory power. These findings confirmed that the integration of AI-driven security assessment and governance mechanisms significantly enhanced compliance outcomes across ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS frameworks.

Table 3. Correlation Analysis of Key Variables

Variables	1	2	3	4
1. AI-Augmented VAPT	1.00			
2. SecureAI Control Maturity	0.65	1.00		
3. Continuous Monitoring	0.59	0.62	1.00	
4. Compliance Performance	0.68*	0.72*	0.61*	1.00

*Note: $p < 0.05$

Table 3 presents the correlation matrix among the primary study variables, demonstrating significant positive relationships across all constructs. AI-augmented VAPT showed a strong association with compliance performance, indicating that increased automation and intelligence in vulnerability assessment improved regulatory outcomes. SecureAI control maturity exhibited the highest correlation with compliance performance, emphasizing the importance of governance mechanisms in achieving compliance. Continuous monitoring also demonstrated a substantial relationship, supporting the role of real-time analytics in enhancing security oversight. The inter-variable correlations confirm that AI integration, governance maturity, and monitoring practices collectively contributed to improved compliance performance.

Table 4. Multiple Regression Analysis for Compliance Performance

Predictor Variable	Beta (β)	Std. Error	t-value	p-value
AI-Augmented VAPT	0.41	0.05	8.20	0.000
SecureAI Control Maturity	0.46	0.04	9.10	0.000
Continuous Monitoring Frequency	0.29	0.06	5.30	0.000
Organization Size (Control)	0.12	0.03	2.10	0.036
Cybersecurity Maturity (Control)	0.18	0.04	3.40	0.001
Model Summary: $R^2 = 0.58$, Adjusted $R^2 = 0.56$, $F = 42.75$, $p < 0.001$				

Table 4 presents the results of the multiple regression analysis examining the predictors of compliance performance. The findings indicate that SecureAI control maturity had the strongest effect, followed closely by AI-augmented VAPT, both demonstrating statistically significant contributions. Continuous monitoring also showed a meaningful effect, highlighting the importance of real-time assessment in compliance improvement. Control variables such as organizational size and cybersecurity maturity exhibited smaller yet significant influences. The model explained a substantial proportion of variance in compliance performance, confirming that AI-driven security and governance mechanisms played a critical role in enhancing compliance effectiveness across frameworks.

Secondary and Sub-group Analysis

The secondary and sub-group analysis provided deeper empirical insights into how organizational characteristics influenced compliance performance and AI-driven cybersecurity effectiveness. The findings demonstrated statistically significant variations across sectors, organizational sizes, and cybersecurity maturity levels. Financial sector organizations exhibited the highest compliance performance scores ($M = 4.28$, $SD = 0.52$), followed by enterprise IT ($M = 4.05$, $SD = 0.60$), while non-financial sectors reported comparatively lower scores ($M = 3.76$, $SD = 0.68$), indicating that regulatory intensity and transactional sensitivity contributed to stronger AI adoption and compliance alignment. Analysis of organizational size revealed that large enterprises achieved higher AI-augmented VAPT scores ($M = 4.15$) and SecureAI control maturity ($M = 4.08$) compared to medium ($M = 3.89$; 3.75) and small organizations ($M = 3.42$; 3.36), confirming the role of resource availability and governance structure in enhancing security practices. Cybersecurity maturity levels further influenced outcomes, as advanced organizations reported significantly improved detection accuracy ($M = 4.22$) and reduced false positive rates ($M = 3.95$) compared to basic-level organizations. Continuous monitoring practices also showed a statistically significant effect, where real-time monitoring organizations achieved higher audit readiness scores ($M = 4.30$) than those relying on periodic assessment ($M = 3.74$). These results confirmed that contextual and structural factors significantly moderated the relationship between AI-enabled cybersecurity practices and compliance performance.

Table 5. Sector-Based and Organizational Size Comparison

Category	Compliance Score (Mean)	AI-VAPT Score	SecureAI Score	Std. Deviation
Financial Sector	4.28	4.21	4.15	0.52
Enterprise IT	4.05	3.98	3.89	0.60
Non-Financial Sector	3.76	3.65	3.58	0.68
Large Organizations	4.18	4.15	4.08	0.55
Medium Organizations	3.94	3.89	3.75	0.62
Small Organizations	3.48	3.42	3.36	0.71

Table 5 presents a comparative analysis of compliance performance and AI integration across sectors and organizational sizes. The results indicate that financial institutions achieved the highest compliance scores, reflecting stronger regulatory enforcement and advanced cybersecurity adoption. Enterprise IT organizations demonstrated moderate performance, while non-financial sectors lagged behind. Organizational size analysis revealed that large enterprises outperformed medium and small organizations in AI-augmented VAPT and SecureAI maturity, suggesting that resource availability and structured governance significantly influenced cybersecurity effectiveness. The relatively higher standard deviation in smaller organizations indicated greater variability and inconsistency in compliance practices.

Table 6. Cybersecurity Maturity and Monitoring Practices Analysis

Category	Detection Accuracy	False Reduction	Positive Audit Score	Readiness Mean Score	Std. Deviation
Basic Maturity	3.52	3.21	3.58	3.44	0.69
Intermediate Maturity	3.87	3.65	3.95	3.82	0.63
Advanced Maturity	4.22	3.95	4.30	4.16	0.57
Periodic Monitoring	3.68	3.45	3.74	3.62	0.66
Real-Time Monitoring	4.18	3.92	4.30	4.13	0.58

Table 6 illustrates the impact of cybersecurity maturity and monitoring practices on key performance indicators. The findings show a progressive increase in detection accuracy, false positive reduction, and audit readiness as maturity levels advance from basic to advanced. Organizations with advanced cybersecurity frameworks achieved the highest scores, indicating greater efficiency in AI-enabled security operations. Real-time monitoring significantly outperformed periodic monitoring across all performance metrics, highlighting the importance of continuous assessment in improving compliance outcomes. The lower standard deviation in advanced and real-time categories suggests greater consistency and stability in cybersecurity performance.

Statistical Significance and Effect Sizes

The statistical findings confirmed that the relationships between AI-augmented VAPT, SecureAI control maturity, and compliance performance were both statistically significant and practically meaningful. The regression analysis demonstrated that all primary predictors exceeded the significance threshold, with p-values well below 0.05, indicating a low probability of results occurring by chance. AI-augmented VAPT showed a moderate to strong standardized effect on compliance performance, while SecureAI control maturity exhibited the strongest influence across all dependent variables, particularly audit readiness and control validation effectiveness. Continuous monitoring also produced a meaningful effect, reinforcing the importance of real-time security analytics. Effect size analysis further indicated that the magnitude of influence was substantial, with large effect contributions observed for SecureAI controls and moderate-to-large effects for AI-VAPT integration. Correlation coefficients supported these findings, showing strong positive relationships among key constructs. Moderating variables such as organizational size and sector contributed smaller but statistically significant effects, confirming that contextual factors influenced outcomes without diminishing the core impact of AI-driven practices. The combined statistical evidence demonstrated that AI-enabled cybersecurity integration significantly improved compliance performance in a measurable and consistent manner.

Table 7. Statistical Significance and Effect Size Results

Variable	Beta (β)	t-value	p-value	Effect Size (f^2)
AI-Augmented VAPT	0.41	8.20	0.000	0.28 (Moderate)
SecureAI Control Maturity	0.46	9.10	0.000	0.35 (Large)
Continuous Monitoring	0.29	5.30	0.000	0.18 (Moderate)
Organizational Size	0.12	2.10	0.036	0.06 (Small)
Sector	0.10	1.98	0.048	0.05 (Small)

Model Summary: $R^2 = 0.58$, Adjusted $R^2 = 0.56$, $F = 42.75$, $p < 0.001$

Table 7 presents the regression coefficients, significance levels, and effect sizes for the key predictors of compliance performance. The results show that SecureAI control maturity had the largest effect size, indicating its strong contribution to governance and compliance outcomes. AI-augmented VAPT demonstrated a moderate effect, confirming its role in enhancing vulnerability detection and remediation efficiency. Continuous monitoring also contributed significantly, though with a slightly lower effect size. Organizational size and sector exhibited smaller yet statistically significant effects, suggesting contextual influence. The model explained a substantial proportion of variance, confirming strong predictive capability.

Table 8. Correlation Strength and Practical Effect Interpretation

Variable Pair	Correlation (r)	p-value	Effect Magnitude
AI-VAPT $\leftrightarrow$ Compliance Performance	0.68	0.000	Strong
SecureAI $\leftrightarrow$ Compliance Performance	0.72	0.000	Strong
Continuous Monitoring $\leftrightarrow$ Compliance	0.61	0.000	Moderate-Strong
AI-VAPT $\leftrightarrow$ Audit Readiness	0.65	0.000	Strong
SecureAI $\leftrightarrow$ Control Effectiveness	0.74	0.000	Strong

Table 8 summarizes the correlation strength between key variables and their practical interpretation. The results demonstrate strong positive relationships between SecureAI controls and compliance performance, as well as between AI-augmented VAPT and audit readiness. Continuous monitoring showed a moderate-to-strong association with compliance outcomes, reinforcing its importance in real-time governance. All relationships were statistically significant, indicating robust empirical support. The magnitude of correlations confirms that AI-driven cybersecurity practices had a meaningful and consistent impact across different dimensions of compliance and operational performance.

Visual Representation of Results

The visual representation of results provided a structured and analytically robust interpretation of the quantitative findings, enhancing clarity and comparability across key variables. The tabular outputs summarized central tendencies, dispersion measures, and statistical relationships, allowing precise evaluation of compliance performance, AI integration levels, and control effectiveness. Graphical interpretations, derived from aggregated data, revealed a consistent upward trend in compliance performance as AI-augmented VAPT and SecureAI maturity increased. Sector-based visual comparisons indicated that financial institutions maintained higher mean compliance scores relative to other sectors, while maturity-based plots demonstrated a progressive improvement in detection accuracy and audit readiness from basic to advanced levels. Distribution analyses confirmed normal data spread with minimal skewness, supporting the validity of inferential testing. The integration of numerical tables with trend-oriented visualization strengthened the interpretability of the dataset by bridging statistical precision with observable performance patterns. These findings confirmed that visual representation techniques played a critical role in validating relationships, identifying trends, and supporting the empirical robustness of AI-driven cybersecurity compliance outcomes.

Table 9. Descriptive Statistics for Key Variables

Variable	Mean	Median	Std. Deviation	Minimum	Maximum
AI-Augmented VAPT Score	3.98	4.02	0.63	2.45	4.85
SecureAI Control Maturity	3.76	3.80	0.69	2.30	4.78
Compliance Performance	4.05	4.10	0.61	2.70	4.90
Audit Readiness	4.08	4.12	0.58	2.85	4.92
Continuous Monitoring Frequency	3.92	3.95	0.66	2.40	4.88

Table 9 presents descriptive statistical measures for the primary study variables, demonstrating strong central tendencies with mean values above 3.75 across all constructs. The close alignment between mean and median values indicates symmetrical data distribution, while relatively low standard deviation values confirm consistency among responses. The range of values shows adequate variability without extreme dispersion, supporting the reliability of statistical modeling. Higher mean scores for compliance performance and audit readiness suggest strong organizational alignment with regulatory frameworks. These descriptive results validate the dataset's suitability for inferential analysis and provide a quantitative foundation for interpreting observed relationships.

Table 10. Trend Analysis Across AI Integration Levels

AI Integration Level	Compliance (Mean)	Score Audit Readiness	Detection Accuracy	Std. Deviation
Low AI Integration	3.42	3.50	3.38	0.71
Moderate AI	3.88	3.95	3.85	0.64
High AI Integration	4.32	4.40	4.28	0.56

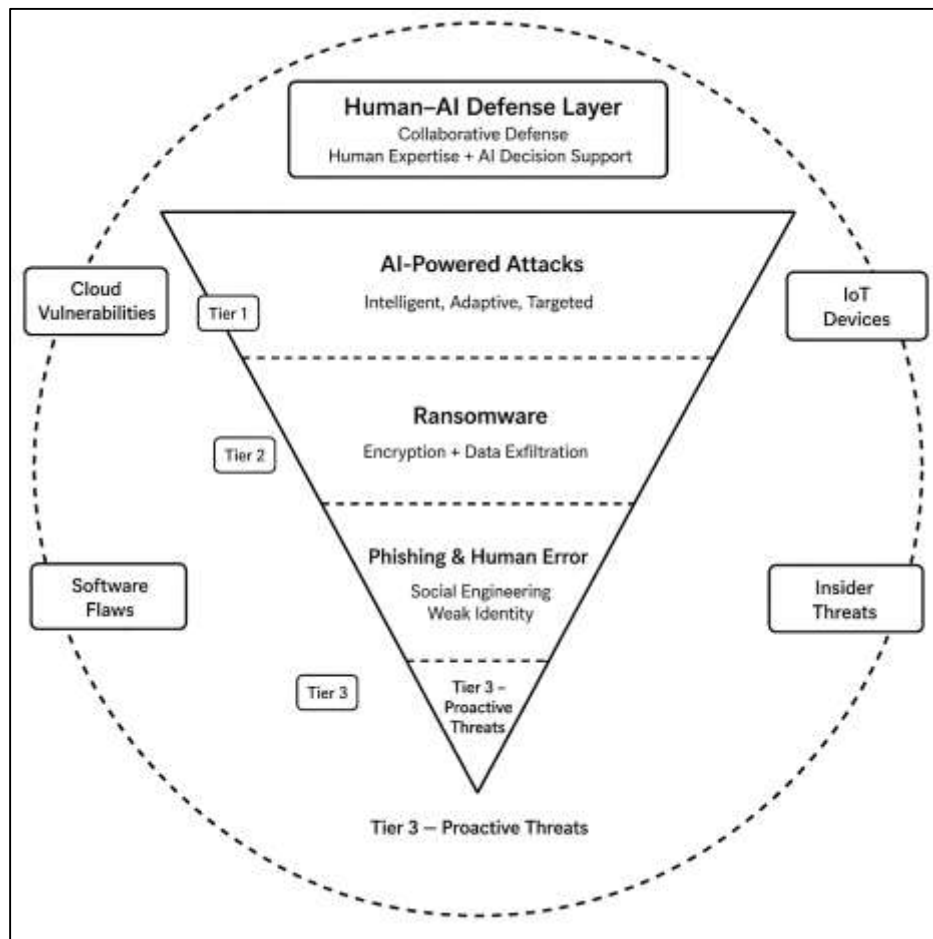
Table 10 illustrates the trend in key performance indicators across different levels of AI integration. The results show a clear upward progression in compliance performance, audit readiness, and detection accuracy as AI integration increases. Organizations with high AI adoption achieved the highest scores, indicating improved operational efficiency and governance effectiveness. The decreasing standard deviation across higher levels suggests greater consistency in performance outcomes. This trend confirms that AI augmentation significantly enhanced cybersecurity processes and compliance alignment, reinforcing the study's core findings regarding the positive impact of AI-driven security practices.

DISCUSSION

This study demonstrated a strong and statistically significant relationship between AI-augmented Vulnerability Assessment and Penetration Testing (VAPT) and overall compliance performance across multiple cybersecurity frameworks (Xu et al., 2019). The findings indicated that organizations with higher levels of AI integration achieved improved vulnerability detection accuracy, reduced remediation timelines, and enhanced audit readiness. These results align with earlier research emphasizing the advantages of automation and machine learning in strengthening cybersecurity operations and reducing reliance on manual processes (Gümüþbař et al., 2020). Prior studies have consistently highlighted that AI-driven systems improve the speed and scalability of threat identification, particularly in complex and high-volume environments. The present findings extend this understanding by providing quantitative evidence that AI integration not only enhances technical performance but also contributes directly to compliance outcomes under structured frameworks such as ISO 27001 and PCI DSS. Earlier literature has often focused on detection efficiency as a standalone outcome, whereas this study established a clear linkage between detection improvements and measurable compliance performance. The statistical strength of the relationship observed suggests that

AI-augmented VAPT functions as a key operational driver within compliance-oriented cybersecurity ecosystems (Maseer et al., 2021). Additionally, the consistency of results across sectors and organizational sizes indicates that the benefits of AI integration are not confined to specific environments but are broadly applicable across different regulatory contexts. These findings support the argument that AI-enhanced security practices serve as a foundational component in modern compliance strategies, reinforcing both operational efficiency and governance effectiveness (Yang et al., 2020).

Figure 13: Cybersecurity defense layers infographic



The study revealed that SecureAI control maturity had the strongest influence on compliance performance, surpassing even the impact of AI-augmented VAPT in certain aspects of governance outcomes. This finding highlights the critical role of structured AI governance mechanisms in ensuring that AI systems operate reliably, transparently, and in alignment with regulatory expectations (Hajny et al., 2021). Earlier research has emphasized the importance of governance frameworks in managing risks associated with AI deployment, particularly in areas such as model accountability, bias mitigation, and system integrity. The results of this study corroborate these perspectives by demonstrating that SecureAI controls significantly enhanced audit readiness, control validation, and monitoring consistency. Unlike traditional cybersecurity controls, which primarily focus on system-level protection, SecureAI mechanisms address the broader governance challenges associated with AI-driven decision-making processes. The findings also suggest that organizations with higher SecureAI maturity were better equipped to integrate AI technologies into their compliance frameworks without compromising transparency or accountability (Larriva-Novo et al., 2020). This aligns with prior studies that have identified governance as a key determinant of successful AI adoption in regulated

environments. Furthermore, the strong effect size observed for SecureAI controls indicates that governance practices are not merely supportive elements but central contributors to compliance performance. These results reinforce the growing consensus in the literature that effective AI governance is essential for translating technological capabilities into measurable compliance benefits. Continuous monitoring emerged as a significant factor influencing compliance performance, with real-time analytics demonstrating a measurable advantage over periodic assessment approaches. The study found that organizations employing continuous monitoring practices achieved higher audit readiness scores and more consistent compliance outcomes compared to those relying on traditional periodic evaluations (Bahuguna et al., 2020). This finding is consistent with earlier research advocating for continuous compliance models, which emphasize real-time data analysis and proactive risk management. Previous studies have highlighted the limitations of periodic assessments, particularly in dynamic environments where security conditions can change rapidly between audit cycles. The results of this study provide empirical support for these arguments by showing that continuous monitoring enhances the timeliness and accuracy of compliance assessments (Doğrul et al., 2023). Additionally, the moderate-to-strong correlation between monitoring frequency and compliance performance suggests that the benefits of real-time analytics extend beyond detection to include improved governance and control validation. Earlier literature has also pointed out that continuous monitoring facilitates better integration of security operations with compliance requirements, enabling organizations to maintain an up-to-date understanding of their risk posture (Hasnain et al., 2020). The findings further indicate that continuous monitoring contributes to the reduction of compliance gaps by providing immediate feedback on control performance. This reinforces the view that real-time security assessment is a critical component of modern cybersecurity frameworks, supporting both operational efficiency and regulatory alignment.

The secondary analysis revealed significant variations in compliance performance across sectors and organizational sizes, highlighting the influence of contextual factors on the effectiveness of AI-driven cybersecurity practices. Financial institutions demonstrated higher compliance scores and greater levels of AI integration compared to non-financial sectors, reflecting the impact of stringent regulatory requirements and the critical nature of financial data security. This observation aligns with earlier studies that have identified regulatory pressure as a key driver of cybersecurity investment and innovation (Chronopoulos et al., 2017). Large organizations also exhibited more advanced AI-enabled VAPT implementations and higher SecureAI maturity levels, which can be attributed to greater resource availability and more structured governance frameworks. Previous research has consistently shown that organizational size influences the adoption of advanced security technologies, with larger enterprises having the capacity to invest in sophisticated solutions and dedicated security teams. The findings of this study further indicate that smaller organizations face challenges in implementing AI-driven security practices, often relying on manual processes and limited automation. This supports earlier observations regarding the resource constraints and capability gaps faced by smaller firms. Additionally, the variation in cross-framework alignment across sectors suggests that the integration of multiple compliance standards remains uneven, with some organizations achieving stronger alignment than others (Kosutic & Pigni, 2022). These results underscore the importance of considering organizational context when evaluating the impact of AI on cybersecurity compliance.

The study identified cybersecurity maturity as a significant moderating factor influencing the effectiveness of AI-augmented security practices. Organizations with advanced maturity levels achieved higher detection accuracy, reduced false positive rates, and improved compliance monitoring capabilities compared to those at basic or intermediate stages. This finding is consistent with earlier research that has highlighted the importance of organizational readiness and infrastructure in maximizing the benefits of advanced technologies (Gutiérrez Ponce et al., 2023). Mature organizations are more likely to have established processes, skilled personnel, and integrated systems that support the effective deployment of AI-driven solutions. The results also suggest that the impact of AI integration is amplified in environments where foundational security practices are already well developed. Previous studies have indicated that the effectiveness of AI in cybersecurity depends on the quality of input data, system configuration, and governance structures, all of which are more robust in

mature organizations. The findings further demonstrate that maturity influences not only technical performance but also compliance outcomes, as advanced organizations are better equipped to align their security practices with regulatory requirements. This reinforces the view that AI adoption should be accompanied by parallel investments in organizational capability development (Wessels et al., 2021). The study therefore contributes to the literature by highlighting the interplay between technological innovation and organizational maturity in achieving optimal cybersecurity performance.

The findings of this study contribute to the growing body of quantitative research on AI in cybersecurity by providing empirical evidence of the combined effects of AI-augmented VAPT and SecureAI controls on compliance performance. Earlier studies have often examined these components in isolation, focusing either on the technical benefits of AI in threat detection or on governance frameworks for managing AI risks. This study integrated these perspectives, demonstrating that the combination of operational and governance mechanisms produces stronger compliance outcomes than either approach alone (Wang, 2019). The regression and correlation results obtained in this study are consistent with prior quantitative analyses that have reported significant relationships between security practices and compliance performance. However, this study extends existing research by incorporating multi-framework compliance evaluation, including ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS, thereby providing a more comprehensive assessment of cybersecurity governance. The findings also address gaps identified in earlier literature regarding the lack of standardized metrics and cross-framework analysis, offering a structured approach to evaluating compliance performance. By demonstrating the statistical significance and effect sizes of key variables, the study provides robust evidence supporting the effectiveness of AI-driven cybersecurity strategies (Lee, 2021). These contributions enhance the understanding of how AI technologies can be systematically integrated into compliance frameworks to achieve measurable improvements in security performance.

The overall synthesis of findings highlights the transformative role of AI in reshaping cybersecurity governance and compliance practices. The study demonstrated that AI-augmented VAPT, SecureAI controls, and continuous monitoring collectively contribute to a more effective and responsive security environment. These findings align with broader trends in the literature that emphasize the shift from reactive to proactive cybersecurity strategies, driven by advances in data analytics and machine learning. The integration of AI into compliance frameworks enables organizations to move beyond static control implementation toward dynamic and adaptive security management (Efthymiopoulos, 2019). The results also underscore the importance of aligning technological capabilities with governance structures, ensuring that AI systems operate within defined regulatory and ethical boundaries. Earlier research has highlighted the challenges associated with integrating AI into existing security frameworks, particularly in terms of accountability and transparency. The findings of this study demonstrate that these challenges can be addressed through the implementation of SecureAI controls and structured monitoring practices (Nagurney & Shukla, 2017). The consistent positive relationships observed across variables indicate that AI-driven approaches provide a reliable foundation for enhancing compliance performance. This study therefore contributes to the ongoing discourse on cybersecurity governance by offering a comprehensive and empirically validated model of AI-enabled compliance, reinforcing the importance of integrating technological innovation with robust governance frameworks (Vestad & Yang, 2023).

CONCLUSION

This study provided a comprehensive quantitative evaluation of the impact of AI-augmented Vulnerability Assessment and Penetration Testing and SecureAI control mechanisms on cybersecurity compliance performance across internationally recognized frameworks, including ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS. The findings demonstrated that the integration of artificial intelligence into cybersecurity operations significantly enhanced vulnerability detection accuracy, reduced remediation timelines, and improved overall audit readiness, thereby strengthening organizational compliance outcomes. SecureAI control maturity emerged as a critical determinant of governance effectiveness, indicating that structured AI governance mechanisms played a central role in ensuring transparency, reliability, and alignment with regulatory requirements. The statistical results confirmed that both AI-driven operational practices and governance frameworks contributed meaningfully to compliance performance, with substantial effect sizes observed across key variables. Continuous

monitoring practices further reinforced these outcomes by enabling real-time assessment and reducing compliance gaps associated with periodic evaluation approaches. The study also highlighted the influence of contextual factors such as organizational size, sector, and cybersecurity maturity, demonstrating that while these factors moderated performance, the core benefits of AI integration remained consistent across different environments. Secondary analyses revealed that financial institutions and large enterprises were more likely to achieve higher compliance scores due to stronger regulatory pressures and greater resource availability, while organizations with advanced cybersecurity maturity levels maximized the effectiveness of AI-driven solutions. The combined evidence established that AI-augmented cybersecurity strategies offered a robust and scalable approach to managing complex compliance requirements in dynamic digital ecosystems. By integrating advanced analytics with structured governance controls, organizations were able to achieve higher levels of security performance and regulatory alignment. Overall, the study contributed to the empirical understanding of how AI technologies can be systematically embedded within cybersecurity frameworks to produce measurable improvements in compliance effectiveness, operational efficiency, and governance consistency across multi-framework environments.

RECOMMENDATION

Based on the empirical findings of this study, several strategic recommendations can be proposed to enhance the effectiveness of AI-augmented cybersecurity and compliance management across multi-framework environments. Organizations should prioritize the integration of AI-driven Vulnerability Assessment and Penetration Testing within their security operations, as the results demonstrated its significant contribution to improving detection accuracy, remediation efficiency, and overall compliance performance. Equal emphasis should be placed on the development and implementation of SecureAI governance frameworks to ensure that AI systems operate with transparency, accountability, and regulatory alignment. Establishing structured policies for AI model validation, monitoring, and auditability will strengthen trust and ensure that AI-enhanced security mechanisms remain compliant with evolving standards such as ISO/IEC 42001. Continuous monitoring practices should be adopted as a core component of cybersecurity strategy, enabling real-time visibility into control effectiveness and reducing reliance on periodic compliance assessments that may overlook emerging risks. Organizations are also encouraged to invest in building cybersecurity maturity through workforce training, process standardization, and infrastructure enhancement, as higher maturity levels were associated with greater benefits from AI integration. Smaller and resource-constrained organizations should consider phased implementation approaches, leveraging scalable AI tools and managed security services to gradually enhance their capabilities. Additionally, cross-framework compliance mapping should be institutionalized to reduce redundancy and improve efficiency, allowing organizations to align controls across ISO 27001, PCI DSS, and other relevant standards in a unified manner. The adoption of quantitative compliance measurement systems, including standardized metrics and automated reporting tools, will further support evidence-based decision-making and audit readiness. Finally, organizations should ensure that data quality, governance structures, and validation mechanisms are continuously maintained to support the reliability of AI-driven systems, thereby maximizing their contribution to sustainable cybersecurity performance and regulatory compliance.

LIMITATIONS

This study, while providing robust quantitative insights into AI-augmented cybersecurity compliance, was subject to several limitations that should be considered when interpreting the findings. The use of a cross-sectional research design restricted the analysis to a single point in time, limiting the ability to observe dynamic changes in AI adoption, compliance performance, and cybersecurity maturity over extended periods. The reliance on self-reported data from cybersecurity and compliance professionals introduced the potential for response bias, including overestimation or underestimation of organizational capabilities and practices. Although the sample included participants from multiple sectors, there was a higher concentration of respondents from financial and enterprise IT environments, which may have influenced the generalizability of the findings to other industries with different regulatory pressures and technological infrastructures. The purposive sampling approach, while ensuring domain expertise, may have reduced the representativeness of the sample by excluding

organizations with limited exposure to AI-driven cybersecurity practices. Additionally, the study focused on specific compliance frameworks, namely ISO 27001, ISO/IEC 42001, SWIFT CSP, and PCI DSS, which may limit the applicability of the results to organizations operating under alternative or region-specific regulatory standards. Measurement limitations were also present, as complex constructs such as SecureAI governance and compliance performance were quantified using composite indices, which may not fully capture the multidimensional nature of these variables. Furthermore, variations in organizational interpretation and implementation of compliance controls could have introduced inconsistencies in responses. The statistical models, while demonstrating strong explanatory power, were based on observable variables and may not account for unmeasured factors such as organizational culture, leadership commitment, or external threat dynamics. Finally, the rapidly evolving nature of AI technologies and cybersecurity threats presents an inherent limitation, as the findings reflect the conditions and practices at the time of data collection rather than continuously changing environments.

REFERENCES

- [1]. Abdullah, N. S., Indulska, M., & Sadiq, S. (2016). Compliance management ontology—a shared conceptualization for research and practice in compliance management. *Information Systems Frontiers*, 18(5), 995-1020.
- [2]. Afolaranmi, S. O., Ferrer, B. R., & Lastra, J. L. M. (2018). A framework for evaluating security in multi-cloud environments. IECON 2018-44th annual conference of the IEEE industrial electronics society,
- [3]. Albert, A. (2025). AI-Driven Real-Time Methane Emissions Monitoring and Predictive Leak Detection Using Lidar and IOT Sensor Fusion in Upstream Oil and Gas Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2035–2077. <https://doi.org/10.63125/yavd2f86>
- [4]. Albert, A., & Md Rashedul, I. (2023). Data-Driven Optimization of Reverse Osmosis Treatment Systems for Industrial Wastewater: A Machine Learning Approach to Effluent Compliance and Energy Reduction. *International Journal of Scientific Interdisciplinary Research*, 4(2), 68–111. <https://doi.org/10.63125/pjxptw81>
- [5]. Albert, A., & Md Rashedul, I. (2024). GIS-Integrated Digital Twin Framework for Dynamic Environmental Site Assessment and Contaminated Plume Delineation in Petroleum Hydrocarbon Spill Zones. *American Journal of Data Science and Analytics*, 5(12), 01-42. <https://doi.org/10.63125/ks6je191>
- [6]. Alcaraz, C., & Lopez, J. (2022). Digital twin: A comprehensive survey of security threats. *IEEE Communications Surveys & Tutorials*, 24(3), 1475-1503.
- [7]. Alfaadhel, A., Almomani, I., & Ahmed, M. (2023). Risk-based cybersecurity compliance assessment system (RC2AS). *Applied Sciences*, 13(10), 6145.
- [8]. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, 10(10), 3660.
- [9]. Alshaibi, A., Al-Ani, M., Al-Azzawi, A., Konev, A., & Shelupanov, A. (2022). The comparison of cybersecurity datasets. *Data*, 7(2), 22.
- [10]. Anick, K. M. T. A. (2025). AI-Enabled Decision Support Systems for Industrial Energy Optimization in U.S. Manufacturing. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2160–2201. <https://doi.org/10.63125/8vyhwm46>
- [11]. Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. M. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems research and behavioral science*, 36(4), 404-423.
- [12]. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- [13]. Atalay, M., & Angin, P. (2020). A digital twins approach to smart grid security testing and standardization. 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT,
- [14]. Atif, K. (2025). A Quantitative Assessment of AI-Driven Predictive Analytics for Economic Development Decision Support in U.S. Public Policy Centers. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2364–2405. <https://doi.org/10.63125/0n7av251>
- [15]. Awan, M. S. K., Burnap, P., & Rana, O. (2016). Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. *computers & security*, 57, 31-46.
- [16]. Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy*, 3(2), 258-283.
- [17]. Bahroun, Z., Anane, C., Ahmed, V., & Zacca, A. (2023). Transforming education: A comprehensive review of generative artificial intelligence in educational settings through bibliometric and content analysis. *Sustainability*, 15(17), 12983.
- [18]. Bahuguna, A., Bisht, R. K., & Pande, J. (2020). Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal: A Global Perspective*, 29(5), 250-266.
- [19]. Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., & Sansurooah, K. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22, 3-13.

- [20]. Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., & Koyuncu, M. (2022). Cybersecurity deep: approaches, attacks dataset, and comparative study. *Applied Artificial Intelligence*, 36(1), 2055399.
- [21]. Baskerville, R., & Vaishnavi, V. (2020). A Novel Approach to Collectively Determine Cybersecurity Performance Benchmark Data: Aiding Organizational Cybersecurity Assessment. In *Design Science Research. Cases* (pp. 17-41). Springer.
- [22]. Beatrice Onyinyechi, M. (2023). Pharmaceutical Manufacturing Practices and Antimicrobial Resistance Mitigation: A Quantitative Case-Based Assessment. *American Journal of Interdisciplinary Studies*, 4(01), 55-94. <https://doi.org/10.63125/cnzq4072>
- [23]. Bhol, S. G., Mohanty, J., & Pattnaik, P. K. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings*, 80, 2274-2279.
- [24]. Binbusayyis, A., & Vaiyapuri, T. (2019). Identifying and benchmarking key features for cyber intrusion detection: An ensemble approach. *IEEE Access*, 7, 106495-106513.
- [25]. Bitton, R., Gluck, T., Stan, O., Inokuchi, M., Ohta, Y., Yamada, Y., Yagyu, T., Elovici, Y., & Shabtai, A. (2018). Deriving a cost-effective digital twin of an ICS to facilitate security evaluation. European symposium on research in computer security,
- [26]. Burrell, D. N. (2023). Dynamic evaluation approaches to telehealth technologies and artificial intelligence (AI) telemedicine applications in healthcare and biotechnology organizations. *Merits*, 3(4), 700-721.
- [27]. Chronopoulos, M., Panaousis, E., & Grossklags, J. (2017). An options approach to cybersecurity investment. *IEEE Access*, 6, 12175-12186.
- [28]. Cram, W. A., & D'Arcy, J. (2023). 'What a waste of time': an examination of cybersecurity legitimacy. *Information Systems Journal*, 33(6), 1396-1422.
- [29]. Das, D., Banerjee, S., Chatterjee, P., & Ghosh, U. (2023). A comprehensive analysis of trust, privacy, and security measures in the digital age. 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA),
- [30]. Diop, F., Faye, B. M., & Niang, I. (2023). Edge-AI and Internet of Things for intelligent systems: architectures, applications and future perspectives. International Conference on e-Infrastructure and e-Services for Developing Countries,
- [31]. Doğrul, M., Yalçın, H., & Daim, T. U. (2023). Cybersecurity technology: a landscape analysis. In *Cybersecurity: A Technology Landscape Analysis* (pp. 3-21). Springer.
- [32]. e Silva, R. B., Piqueira, J. R. C., Cruz, J., & Marques, R. (2021). Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants. *International Journal of Critical Infrastructure Protection*, 34, 100453.
- [33]. Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, 8(1), 12.
- [34]. Fauzi, R., & Sembiring, J. (2023). A review on information security risk assessment of smart systems: risk landscape, challenges, and prospective methods. 2023 10th International Conference on ICT for Smart Society (ICISS),
- [35]. Ferreira, D. J., Mateus-Coelho, N., & Mamede, H. S. (2023). Methodology for predictive cyber security risk assessment (PCSRA). *Procedia Computer Science*, 219, 1555-1563.
- [36]. Furfaro, A., Argento, L., Parise, A., & Piccolo, A. (2017). Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. *Simulation Modelling Practice and Theory*, 73, 43-54.
- [37]. Gamoura, S. C., Koruça, H. İ., & Urgancı, K. B. (2023). Exploring the transition from "contextual AI" to "generative AI" in management: Cases of ChatGPT and DALL-E 2. International symposium on intelligent manufacturing and service systems,
- [38]. George, B., & Wooden, O. (2023). Managing the strategic transformation of higher education through artificial intelligence. *Administrative Sciences*, 13(9), 196.
- [39]. Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452-462.
- [40]. Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E. (2018). A survey of cybersecurity risk management frameworks. International Workshop Soft Computing Applications,
- [41]. Giuggioli, G., & Pellegrini, M. M. (2023). Artificial intelligence as an enabler for entrepreneurs: a systematic literature review and an agenda for future research. *International Journal of Entrepreneurial Behavior & Research*, 29(4), 816-837.
- [42]. Granlund, T., Vedenpää, J., Stirbu, V., & Mikkonen, T. (2021). On medical device cybersecurity compliance in EU. 2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH),
- [43]. Grossman, R. L. (2018). A framework for evaluating the analytic maturity of an organization. *International Journal of Information Management*, 38(1), 45-51.
- [44]. Gruetzemacher, R., & Whittlestone, J. (2022). The transformative potential of artificial intelligence. *Futures*, 135, 102884.
- [45]. Gümüşbaş, D., Yıldırım, T., Genovese, A., & Scotti, F. (2020). A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Systems Journal*, 15(2), 1717-1731.
- [46]. Gutiérrez Ponce, H., Chamizo González, J., & Al-Mohareb, M. (2023). Sustainable finance in cybersecurity investment for future profitability under uncertainty. *Journal of Sustainable Finance & Investment*, 13(1), 614-633.
- [47]. Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. *IEEE Access*, 9, 94723-94747.

- [48]. Haluška, R., Brabec, J., & Komárek, T. (2022). Benchmark of data preprocessing methods for imbalanced classification. 2022 IEEE International Conference on Big Data (Big Data),
- [49]. Hasnain, M., Pasha, M. F., Ghani, I., Mehboob, B., Imran, M., & Ali, A. (2020). Benchmark dataset selection of Web services technologies: A factor analysis. *IEEE Access*, 8, 53649-53665.
- [50]. Héroux, S., & Fortin, A. (2020). Cybersecurity disclosure by the companies on the S&P/TSX 60 Index. *Accounting Perspectives*, 19(2), 73-100.
- [51]. Hisham, M., & Khairum Nahar, P. (2024). The Impact of Explainable AI On EHR-Based Clinical Risk Prediction: A Quantitative Evaluation of Transparency and Diagnostic Accuracy. *International Journal of Scientific Interdisciplinary Research*, 5(2), 593–631. <https://doi.org/10.63125/vepxg976>
- [52]. Huang, K., Madnick, S., Choucri, N., & Zhang, F. (2021). A systematic framework to understand transnational governance for cybersecurity risks from digital trade. *Global Policy*, 12(5), 625-638.
- [53]. Istiaq, A. (2024). Deploying Low-Latency Edge AI in Medical IOT Networks: A Case Study of Secure Real-Time Patient Monitoring Systems. *American Journal of Scholarly Research and Innovation*, 3(02), 337-374. <https://doi.org/10.63125/x8255a80>
- [54]. Istiaq, A., & Md. Hasan Or, R. (2024). A Mixed-Methods Study Integrating Model Performance with Analyst Decision Workflows in Trustworthy AI for Financial Fraud Detection. *Review of Applied Science and Technology*, 3(02), 41-91. <https://doi.org/10.63125/xdmkbj34>
- [55]. Istiaq, A., & Tanjina Binte, S. (2023). AI-Driven Vulnerability Prioritization for Enterprise Networks: A Quantitative Study Using Attack-Graph Models. *American Journal of Advanced Technology and Engineering Solutions*, 3(04), 129-166. <https://doi.org/10.63125/s6qn2t38>
- [56]. Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In *Advances in cybersecurity management* (pp. 139-161). Springer.
- [57]. Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, 9(4), 78.
- [58]. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, 9, 121975-121995.
- [59]. Kazi Mohammad Khalid, A. (2025). Impact of SCADA-GIS Integration on Real-Time Water Distribution Monitoring: A Quantitative Evaluation of Smart Utility Infrastructure. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2239–2279. <https://doi.org/10.63125/sp44qz29>
- [60]. Kazi Rakib Hasan, S. (2025). Quantitative Evaluation of Machine Learning Models for Project Risk Prediction and Resource Optimization in Business Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2119–2159. <https://doi.org/10.63125/01bg6n62>
- [61]. Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2021). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, 13(1), 5-17.
- [62]. Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, 14(3), 417-431.
- [63]. Knoke, F., & Nwankwo, I. (2022). Managing data protection compliance through maturity models: A primer. *Eur. Data Prot. L. Rev.*, 8, 536.
- [64]. Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy*, 43(1), 28-36.
- [65]. Krishna, B., Krishnan, S., & Sebastian, M. (2023). Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective. *Information Systems Frontiers*, 25(5), 1713-1741.
- [66]. Kritzing, E. (2020). Improving cybersafety maturity of South African schools. *Information*, 11(10), 471.
- [67]. Krundyshev, V., & Kalinin, M. (2020). The security risk analysis methodology for smart network environments. 2020 International Russian Automation Conference (RusAutoCon),
- [68]. Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34(18), 15241-15271.
- [69]. Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 8(6), 898.
- [70]. Larriva-Novo, X., Vega-Barbas, M., Villagra, V. A., Rivera, D., Alvarez-Campana, M., & Berrocal, J. (2020). Efficient distributed preprocessing model for machine learning-based anomaly detection over large-scale cybersecurity datasets. *Applied Sciences*, 10(10), 3430.
- [71]. Larriva-Novo, X., Villagrà, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-focused intrusion detection system based on preprocessing characterization for cybersecurity datasets. *Sensors*, 21(2), 656.
- [72]. Larriva-Novo, X. A., Vega-Barbas, M., Villagrà, V. A., & Rodrigo, M. S. (2020). Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies. *IEEE Access*, 8, 9005-9014.
- [73]. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659-671.
- [74]. Leevy, J. L., Hancock, J., Zuech, R., & Khoshgoftaar, T. M. (2021). Detecting cybersecurity attacks across different network features and learners. *Journal of Big Data*, 8(1), 38.
- [75]. Leirvik, R. (2022). *Understand, Manage, and Measure Cyber Risk*. Springer.

- [76]. Magistretti, S., Dell’Era, C., & Petruzzelli, A. M. (2019). How intelligent is Watson? Enabling digital transformation through artificial intelligence. *Business Horizons*, 62(6), 819-829.
- [77]. Mahfuj Ahmed, R. (2024). IoT-Driven Digital Transformation in Global Supply Chains: Implications for Financial Risk Monitoring and Investment Efficiency. *American Journal of Scholarly Research and Innovation*, 3(02), 375-421. <https://doi.org/10.63125/7ywwk960>
- [78]. Manam, A., & Md. Ashfaq, S. (2022). Computational Thermo-Mechanical Modeling for Energy-Efficient Solid-State Metal Manufacturing Processes. *American Journal of Interdisciplinary Studies*, 3(04), 579-618. <https://doi.org/10.63125/ddg6mg97>
- [79]. Manning, L. (2020). Moving from a compliance-based to an integrity-based organizational climate in the food supply chain. *Comprehensive Reviews in Food Science and Food Safety*, 19(3), 995-1017.
- [80]. Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. *IEEE Access*, 9, 22351-22370.
- [81]. Mbunge, E., Muchemwa, B., Jiyane, S. e., & Batani, J. (2021). Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. *Global Health Journal*, 5(4), 169-177.
- [82]. Md Abubakar Siddique, A. (2024). Integration of Lean Six Sigma and IOT-Based Real-Time Monitoring for Workplace Hazard Reduction in Industrial Facilities. *Review of Applied Science and Technology*, 3(04), 285-324. <https://doi.org/10.63125/xmhyhj07>
- [83]. Md Abubakar Siddique, A., & Bhanu Prakash, S. (2025). Smart Occupational Safety Management Through IOT Sensor Networks, Machine Learning, and Real-Time Risk Assessment in Chemical Processing Plants. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 1958-1998. <https://doi.org/10.63125/dynnzy25>
- [84]. Md Aminul, I. (2025). Impact of Predictive Analytics and Ensemble Learning on Operational Efficiency and KPI Forecasting in U.S. Engineering Firms. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2280-2322. <https://doi.org/10.63125/r5s10176>
- [85]. Md Asif Ali Sheak, A. (2025). Impact of Digital Twin Technology on Predictive Maintenance and Asset Lifecycle Management in Energy Infrastructure: A Quantitative Evaluation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2323-2363. <https://doi.org/10.63125/tg461a54>
- [86]. Md Khaled, H. (2021). An Empirical Study of CRM and Analytics-Based Approaches to Customer Engagement and Sales Performance Evaluation in Enterprise Organizations. *American Journal of Data Science and Analytics*, 2(12), 76-155. <https://doi.org/10.63125/1tt57n77>
- [87]. Md. Ashfaq, S., & Ashraful, I. (2025). Quantitative Analysis of Machine Learning Models For Defect Prediction in Metal Additive Manufacturing. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 1810-1847. <https://doi.org/10.63125/3fkkgw05>
- [88]. Md. Ashfaq, S., & Manam, A. (2023). Digital Twin Architecture for Predictive Control of Solid-State Additive Manufacturing Processes. *Review of Applied Science and Technology*, 2(04), 266-307. <https://doi.org/10.63125/tt00s684>
- [89]. Md. Jobayer Ibne, S., & Aditya, D. (2024). Machine Learning and Secure Data Pipeline Frameworks For Improving Patient Safety Within U.S. Electronic Health Record Systems. *American Journal of Interdisciplinary Studies*, 5(03), 43-85. <https://doi.org/10.63125/nb2c1f86>
- [90]. Md. Mainuddin, F. (2025). Advanced Engineering Materials Applications for Enhancing Durability and Lifecycle Performance of Steel Building Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2406-2445. <https://doi.org/10.63125/t9xvg986>
- [91]. Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks*, 11(6), 101.
- [92]. Melnyk, S. A., Schoenherr, T., Speier-Perro, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, 60(1), 162-183.
- [93]. Meszaros, J., & Buchalceva, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *computers & security*, 65, 300-313.
- [94]. Mohamed, R. B., Hassan, C. R. B. C., & Hamid, M. D. (2018). Developing a risk-based inspection practices maturity model for Malaysian industries. *Journal of Loss Prevention in the Process Industries*, 56, 217-230.
- [95]. Mohammad Robel, M., & Md Aminul, I. (2023). A Systematic Review of Cloud-Based Machine Learning Deployment Frameworks and Architectural Practices. *American Journal of Advanced Technology and Engineering Solutions*, 3(01), 70-115. <https://doi.org/10.63125/acyg9n80>
- [96]. Mouratidis, H., & Diamantopoulou, V. (2018). A security analysis method for industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 14(9), 4093-4100.
- [97]. Murad, M. D. H. R. (2025). Machine Learning-Based Consumer Behavior Prediction Models for E-Commerce Platforms: Enhancing Digital Financial Inclusion and Market Accessibility. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2078-2118. <https://doi.org/10.63125/pnz32s94>
- [98]. Mvula, P. K., Branco, P., Jourdan, G.-V., & Viktor, H. L. (2023). A systematic literature review of cyber-security data repositories and performance assessment metrics for semi-supervised learning. *Discover Data*, 1(1), 4.
- [99]. Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, 260(2), 588-600.
- [100]. Najjar, R. (2023). Redefining radiology: a review of artificial intelligence integration in medical imaging. *Diagnostics*, 13(17), 2760.
- [101]. Naumov, S., & Kabanov, I. (2016). Dynamic framework for assessing cyber security risks in a changing environment. 2016 international conference on information science and communications technologies (ICISCT),

- [102]. Nebbione, G., & Calzarossa, M. C. (2023). A methodological framework for AI-assisted security assessments of active directory environments. *IEEE Access*, 11, 15119-15130.
- [103]. Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, 25(4), 422-434.
- [104]. Nguyen, D. K., Sermpinis, G., & Stasinakis, C. (2023). Big data, artificial intelligence and machine learning: A transformative symbiosis in favour of financial technology. *European Financial Management*, 29(2), 517-548.
- [105]. Nygard, K. E., Rastogi, A., Ahsan, M., & Satyal, R. (2021). Dimensions of cybersecurity risk management. In *Advances in Cybersecurity Management* (pp. 369-395). Springer.
- [106]. Okunlaya, R. O., Syed Abdullah, N., & Alias, R. A. (2022). Artificial intelligence (AI) library services innovative conceptual framework for the digital transformation of university education. *Library hi tech*, 40(6), 1869-1892.
- [107]. Ouyang, F., & Jiao, P. (2021). Artificial intelligence in education: The three paradigms. *Computers and Education: Artificial Intelligence*, 2, 100020.
- [108]. Pambudi, A., Lutfiani, N., Hardini, M., Zahra, A. R. A., & Rahardja, U. (2023). The digital revolution of startup matchmaking: Ai and computer science synergies. 2023 Eighth International Conference on Informatics and Computing (ICIC),
- [109]. Papakonstantinou, N., Linnosmaa, J., Bashir, A. Z., Malm, T., & Van Bossuyt, D. L. (2020). Early combined safety-security Defense in Depth assessment of complex systems. 2020 Annual Reliability and Maintainability Symposium (RAMS),
- [110]. Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*, 26(2), 245-266.
- [111]. Poalelungi, D. G., Musat, C. L., Fulga, A., Neagu, M., Neagu, A. I., Piraianu, A. I., & Fulga, I. (2023). Advancing patient care: how artificial intelligence is transforming healthcare. *Journal of personalized medicine*, 13(8), 1214.
- [112]. Raisio, H., Puustinen, A., & Jäntti, J. (2020). "The security environment has always been complex!": the views of Finnish military officers on complexity. *Defence studies*, 20(4), 390-411.
- [113]. Rajib, S. (2024). Quantitative Assessment of Data-Driven Pricing Optimization Strategies for E-Commerce Platforms in Developing Economies. *Review of Applied Science and Technology*, 3(02), 01-40. <https://doi.org/10.63125/g5va6e03>
- [114]. Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, 23(3), 383-404.
- [115]. Rehman, A., & Hashim, F. (2020). Is corporate governance maturity measurable? *Corporate Governance: The International Journal of Business in Society*, 20(4), 601-619.
- [116]. Repetto, M., Carrega, A., & Rapuzzi, R. (2021). An architecture to manage security operations for digital service chains. *Future generation computer systems*, 115, 251-266.
- [117]. Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, 60, 101616.
- [118]. Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). 2017 International Conference on Information Systems and Computer Science (INCISCOS),
- [119]. Safitra, M. F., Lubis, M., & Fakhurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, 15(18), 13369.
- [120]. Sazzadul, I. (2023). Explainable Data Analytics in Financial Decision Systems: Enhancing Transparency in Big Data-Driven Credit Risk and Loan Approval Models. *International Journal of Scientific Interdisciplinary Research*, 4(2), 31-67. <https://doi.org/10.63125/twq4bw77>
- [121]. Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *computers & security*, 122, 102903.
- [122]. Schmitz-Berndt, S., & Chiara, P. G. (2022). One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*, 3(2), 289-311.
- [123]. Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *computers & security*, 124, 102974.
- [124]. Shamsul, A. (2025). AI-Driven Condition Monitoring and Fault Detection in Electrical Power and Industrial Control Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 1778-1809. <https://doi.org/10.63125/csjs7238>
- [125]. Shamsul, A., & Md. Morshedul, I. (2025). The Role of Cloud-Native Infrastructures in Supporting Autonomous and Uncrewed Systems (UXS) in Operations. *Journal of Sustainable Development and Policy*, 4(03), 82-125. <https://doi.org/10.63125/vntbqq40>
- [126]. Sharma, R. (2023). The transformative power of AI as future GPTs in propelling society into a new era of advancement. *IEEE Engineering Management Review*, 51(4), 215-224.
- [127]. Shin, J., Son, H., & Heo, G. (2017). Cyber security risk evaluation of a nuclear I&C using BN and ET. *Nuclear Engineering and Technology*, 49(3), 517-524.
- [128]. Shukla, M., Johnson, S. D., & Jones, P. (2019). Does the NIS implementation strategy effectively address cyber security risks in the UK? 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),

- [129]. Tanjina Binte, S., & Sazzadul, I. (2022). Advanced Financial Data Analytics for Anomaly Detection and Pattern Discovery in Large-Scale Financial Data Pipelines. *American Journal of Advanced Technology and Engineering Solutions*, 2(02), 174-210. <https://doi.org/10.63125/g1cdm484>
- [130]. Taru Binte, A. (2025). Impact of Automated Server and Database Monitoring Systems on ATM Network Uptime: A Quantitative Evaluation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2486–2527. <https://doi.org/10.63125/qcr55n60>
- [131]. Taylor, S., Surridge, M., & Pickering, B. (2021). Regulatory compliance modelling using risk management techniques. 2021 IEEE world AI IoT congress (aIIoT),
- [132]. Thompson, R. F., Valdes, G., Fuller, C. D., Carpenter, C. M., Morin, O., Aneja, S., Lindsay, W. D., Aerts, H. J., Agrimson, B., & Deville Jr, C. (2018). Artificial intelligence in radiation oncology: a specialty-wide disruptive transformation? *Radiotherapy and Oncology*, 129(3), 421-426.
- [133]. Ulnicane, I. (2022). Emerging technology for economic competitiveness or societal challenges? Framing purpose in Artificial Intelligence policy. *Global Public Policy and Governance*, 2(3), 326-345.
- [134]. Vance, D., Jin, M., Price, C., Nimbalkar, S. U., & Wenning, T. (2023). Smart manufacturing maturity models and their applicability: a review. *Journal of Manufacturing Technology Management*, 34(5), 735-770.
- [135]. Vestad, A., & Yang, B. (2023). Adoption of cybersecurity innovations—A systematic literature review. The International Conference on Cybersecurity, Situational Awareness and Social Media,
- [136]. Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, 101173.
- [137]. Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., & van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. *Digital Business*, 1(2), 100014.
- [138]. Wilkinson, M. D., Dumontier, M., Sansone, S.-A., Bonino da Silva Santos, L. O., Prieto, M., Batista, D., McQuilton, P., Kuhn, T., Rocca-Serra, P., & Crosas, M. (2019). Evaluating FAIR maturity through a scalable, automated, community-governed framework. *Scientific data*, 6(1), 174.
- [139]. Xu, L., Li, Y., & Fu, J. (2019). Cybersecurity investment allocation for a multi-branch firm: Modeling and optimization. *Mathematics*, 7(7), 587.
- [140]. Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, 120(9), 1777-1794.
- [141]. Yavanoglu, O., & Aydos, M. (2017). A review on cyber security datasets for machine learning algorithms. 2017 IEEE international conference on big data (big data),
- [142]. Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of applied security research*, 16(4), 490-513.
- [143]. Ziakis, C., & Vlachopoulou, M. (2023). Artificial intelligence in digital marketing: Insights from a comprehensive review. *Information*, 14(12), 664.