American Journal of Innovation in Science and Engineering (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 5 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 5 Issue 1, Year 2026
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v5i1.7223
https://journals.e-palli.com/home/index.php/ajise

Audit to Assurance: Evaluating the Impact of Regulatory Cybersecurity Audits on Organisational Cyber Resilience and Strategic Decision-Making

Yasir Majeed[1*], Anas Majeed[2]

Article Information

Received: November 21, 2025

Accepted: March 08, 2026

Published: April 11, 2026

Keywords

Audit assurance, Board governance, Cyber resilience, Cybersecurity audit, Enterprise risk management, Information security, Regulatory compliance, Strategic decision-making, Structural equation modelling

ABSTRACT

As digital threats proliferate in scope and sophistication, regulatory bodies worldwide have expanded mandatory cybersecurity audit frameworks to compel organisational accountability. Despite widespread regulatory adoption, evidence on whether compliance translates into genuine cyber resilience remains contested. This study investigates the multidimensional impact of regulatory cybersecurity audits on cyber resilience and strategic decision-making, and introduces the Audit-to-Assurance (A2A) Framework. A mixed-methods design integrates quantitative survey data from 347 enterprise organisations across 12 sectors (hierarchical regression; structural equation modelling) with 24 executive interviews (thematic analysis). Audit intensity ($\beta = 0.42$, $p < .001$) and audit quality ($\beta = 0.61$, $p < .001$) are significant predictors of cyber resilience and strategic outcomes respectively. Remediation depth mediates the audit quality–resilience relationship (indirect effect $\beta = 0.31$, 95% CI [0.24, 0.39]). Board cybersecurity literacy significantly moderates the audit–strategy pathway ($\beta = 0.29$, $p = .002$). All ten hypotheses are supported. Regulatory audits generate substantial resilience and strategic value, but only under conditions of high audit quality, rigorous gap analysis, and deep remediation. The A2A Framework provides a structured roadmap for practitioners and regulators.

INTRODUCTION

The convergence of state-sponsored cyber espionage, ransomware-as-a-service ecosystems, and critical infrastructure vulnerabilities has accelerated the globalisation of mandatory cybersecurity audit regimes (Von Solms and Van Niekerk, 2013; World Economic Forum, 2022). From the European Union's NIS2 Directive and Digital Operational Resilience Act (DORA) (European Parliament and Council, 2022a, 2022b), to the US Securities and Exchange Commission's 2023 cybersecurity disclosure rules (U.S. SEC, 2023), Australia's Security of Critical Infrastructure Act (Australian Government, 2022), and the Kingdom of Saudi Arabia's (KSA) dual-regulator framework comprising the Saudi Central Bank (SAMA) Cyber Security Framework (SAMA, 2017) and the National Cybersecurity Authority's (NCA) Essential Cybersecurity Controls (NCA, 2018), organisations now operate within an expansive and increasingly global regulatory accountability architecture. These frameworks share a common presumption: that structured external audit of cybersecurity controls will produce improved security outcomes (Gordon & Loeb, 2002; OECD, 2015).

This presumption is empirically contestable. Ponemon Institute (2023) reported that 58% of audit-compliant organisations experienced at least one significant breach within 18 months of certification, and Security Scorecard (2020) found that HIPAA-compliant healthcare organisations were no less breach-prone than non-compliant peers. This divergence between compliance status and security outcomes defines what this paper terms the compliance-assurance gap — the distance between satisfying the letter of a regulatory audit requirement and achieving the genuine organisational capability to withstand, respond to, and recover from cyber incidents (Hausken, 2017; Schatz & Bashroush, 2017).

The mechanisms that determine whether regulatory audits close or perpetuate this gap remain underexplored. Existing scholarship has examined cybersecurity investment optimisation (Gordon & Loeb, 2002), compliance motivation (Bulgurcu, Cavusoglu and Benbasat, 2010), and board-level governance (Williams & Hardy, 2020), but has not systematically mapped the multi-stage process by which audit conduct translates or fails to translate into cyber resilience and strategic improvement. This study fills that gap by advancing three contributions.

First, this paper introduces the Audit-to-Assurance (A2A) Framework, a theoretically grounded model that maps regulatory audit conduct through gap analysis and remediation to cyber resilience and strategic decision-making outcomes, with explicit moderating variables. Second, it tests ten hypotheses derived from the A2A Framework using hierarchical regression and structural equation modelling on a sample of 347 senior cybersecurity executives across 12 industry sectors. Third, it derives actionable recommendations for regulators, auditors, and organisational leaders seeking to maximise audit value beyond compliance theatre.

The aim of the study is

To investigate the multidimensional impact of regulatory

[1] The University of Lahore
[2] Victoria University
[*] Corresponding author's e-mail: yasirmajeedsatti@gmail.com

cybersecurity audits on two interlinked organisational outcomes, cyber resilience and strategic decision-making and to identify the conditions under which regulatory audit compliance translates into genuine organisational security improvement.

The study is fundamentally motivated by what it calls the compliance-assurance gap the observed disconnect between an organisation passing a regulatory cybersecurity audit and actually becoming more resilient. As the paper notes, 58% of audit-compliant organisations still experienced a significant breach within 18 months of certification, which raises the core question the study answers: under what conditions do regulatory audits produce genuine security improvement, and under what conditions do they produce only compliance theatre?

LITERATURE REVIEW

Regulatory Cybersecurity Audits

A cybersecurity audit is defined by ISACA (2022, p. 47) as a systematic, independent examination of an organisation's cybersecurity controls, policies, procedures, and capabilities against a defined standard or regulatory requirement. Cybersecurity audits differ from vulnerability assessments and penetration tests in their governance and compliance scopeBaskerville, Spagnoletti, & Kim, 2014). The global regulatory landscape has converged toward mandatory annual audit regimes, with frameworks varying in prescriptiveness from rules-based (PCI DSS v4.0; Payment Card Industry Security Standards Council, 2022) to principles-based (NIST CSF; National Institute of Standards and Technology, 2018) approaches.

Within the Gulf Cooperation Council (GCC) region, the Kingdom of Saudi Arabia has established one of the most comprehensive and rapidly maturing mandatory cybersecurity audit ecosystems globally, driven by the Vision 2030 national transformation agenda. The SAMA Cyber Security Framework (SAMA CSF), published in 2017, mandates annual domain-based maturity assessments across 145 controls for all licensed financial institutions including banks, insurers, and, from 2021, fintech entities operating under the Open Banking Security Framework (SAMA, 2017, 2021). Concurrently, the National Cybersecurity Authority (NCA), established by Royal Decree in 2017, issued the Essential Cybersecurity Controls (ECC-1:2018), a mandatory framework of 141 controls across eight domains applicable to all government entities and critical national infrastructure operators (NCA, 2018). Both frameworks employ a five-level maturity model (L1 = Initial to L5 = Optimising), mandating not merely compliance documentation but time-bound remediation plans tracked through regulatory registers a design feature that distinguishes the KSA regime from many Western counterparts and is examined in this study as an instance of prescriptive regulatory specificity (H4). The NCA further strengthened audit quality in 2023 through the publication of the Cybersecurity Audit Methodology (CCC), standardising audit procedures and third-party auditor accreditation criteria across all covered entities (NCA, 2023).

Audit intensity encompassing audit frequency and scope breadth has been theorised as a primary driver of security improvement through repeated structured assessment (Makridis & Smeets, 2019). More frequent audits create organisational learning cycles (Argyris & Schon, 1978) that embed security awareness into institutional routines and progressively improve control maturity (Schlienger & Teufel, 2003; Tsohou *et al.*, 2015). Evidence from the KSA context supports this mechanism longitudinally: cross-sector cyber resilience scores across SAMA- and NCA-covered entities increased from a mean of approximately 30.2 in 2017 when mandatory audit cycles first commenced to an estimated 69.4 by 2024, a 129.8% improvement attributable in substantial part to the progressive maturity compounding effect of seven consecutive annual audit cycles (Al-Hakami, Bandar and Nisbet, 2020; ISACA, 2023). The discovery function of external audits surfacing vulnerabilities normalised by internal teams further amplifies the intensity-resilience relationship (Lévesque *et al.*, 2017).

H1: Regulatory audit intensity (frequency and scope) is positively and significantly associated with organisational cyber resilience.

H2: Greater audit scope breadth (number of control domains examined) is positively associated with improved cyber resilience outcomes.

Audit Quality and Strategic Outcomes

Audit quality operationalised as the degree of auditor sector expertise, comprehensiveness of control testing, and action ability of remediation guidance determines the strategic value of audit outputs (Gordon, Loeb, Lucyshyn and Sohail, 2020; Kankanhalli *et al.*, 2003). High-quality audits produce business-contextualised findings that translate technical control gaps into financial exposure estimates, enabling C-suite and board engagement with cybersecurity as a strategic risk rather than a technical compliance matter (Ashenden and Sasse, 2013; Cram, Proudfoot and D'Arcy, 2019).

The legitimising function of external audits their capacity to lend institutional authority to security recommendations that internal assessments cannot is particularly salient in the strategic decision-making domain (Hu, Hart and Cooke, 2007). Institutional theory (DiMaggio and Powell, 1983) predicts that coercive regulatory audit findings trigger normative internalisation among board members and C-suite executives, producing strategic cybersecurity investment decisions that would not arise from internal risk assessments alone (Srinidhi, Yan and Bhargava, 2015).

H3: Regulatory audit quality (auditor expertise and actionability of findings) is positively and significantly associated with strategic cybersecurity decision-making integration.

H4: Regulatory regime specificity (prescriptiveness of audit standards) positively moderates the relationship between audit quality and gap analysis rigour.

Gap Analysis, Remediation, and Cyber Resilience

The gap analysis stage mapping audit findings to business-contextualised risk priorities is the critical link between audit conduct and resilience improvement (Huang & Behara, 2013; Liu, Ji and Mookerjee, 2011). Organisations that integrate gap analysis with enterprise risk management processes achieve higher remediation completion rates and more targeted security investment (Bodin, Gordon, and Loeb, 2008; Sveen, Torres, and Sarriegi, 2009). The World Economic Forum (2022, 2023) defines cyber resilience across four dimensions anticipatory, resistance, recovery, and adaptive capacity all of which are amenable to structured improvement through audit-driven gap analysis and remediation.

Remediation depth the extent to which organisations address root causes rather than minimally closing audit findings is established as the proximate driver of resilience improvement (Siponen & Vance, 2010; Safa, Von Solms and Furnell, 2016). Puhakainen and Siponen (2010) demonstrated through action research that deep, integrated remediation produces substantially superior and more durable security improvements than shallow compliance-oriented remediation. Organisational learning theory (Argyris & Schon, 1978) predicts that deep remediation triggers double-loop learning systemic revision of organisational security norms rather than single-loop adjustment of specific controls.

H5: Gap analysis rigour mediates the relationship between audit intensity and cyber resilience, such that more intense audits improve resilience through more rigorous gap analysis.

H6: Remediation depth mediates the relationship between audit quality and cyber resilience, such that higher-quality audits improve resilience through deeper, more integrated remediation.

Moderating Effects: Organisational Size and Board Literacy

Organisational size shapes both the resource availability for audit-driven remediation and the organisational complexity that can impede it (Yildirim *et al.*, 2011; Chang & Ho, 2006). Larger organisations possess greater security investment capacity and more formalised governance structures, amplifying the resilience effects of high audit intensity (Brecht & Nowey, 2013). However, they also face greater coordination challenges in translating audit findings into organisation-wide remediation action, creating a moderating rather than simply additive size effect (Whitman, 2003; Flores, Antonsen and Ekstedt, 2014).

Board cybersecurity literacy the degree to which board members possess substantive cybersecurity knowledge is the theoretically strongest moderator of the audit-to-strategic-decision pathway (Williams & Hardy, 2020; ISACA, 2023). Agency theory (Jensen & Meckling, 1976) predicts that information asymmetry between CISOs and boards impedes the translation of audit intelligence into strategic action; board cybersecurity literacy resolves this asymmetry by enabling board members to interpret, evaluate, and act on audit findings without exclusive reliance on management-filtered information (Cram, Proudfoot and D'Arcy, 2019).

H7: Organisational size positively moderates the relationship between audit intensity and remediation depth, such that the effect of audit intensity on remediation is stronger in larger organisations.

H8: Board cybersecurity literacy positively moderates the relationship between audit quality and strategic decision-making integration, such that audit quality has a stronger effect on strategic decisions in organisations with higher board cyber literacy.

Strategic Decision-Making and Resilience Feedback

Strategic cybersecurity decision-making comprising budget reallocation, governance restructuring, CISO empowerment, and risk-informed strategic planning is both an outcome of the audit-to-assurance transformation and an antecedent of sustained resilience improvement (Srinidhi, Yan and Bhargava, 2015; Gordon, Loeb and Sohail, 2010). Campbell *et al.* (2003) and Cavusoglu, Mishra and Raghunathan (2004) demonstrated that market-disciplined cybersecurity investment, triggered by incident disclosure or audit findings, is associated with durable resilience improvements that persist across subsequent measurement periods.

The feedback loop from strategic decision-making to resilience is theorised as operating through two mechanisms: resource allocation (directing security investment toward highest-risk gaps identified by audit) and governance strengthening (formalising cybersecurity in board agendas, committee structures, and executive accountabilities) (Williams & Hardy, 2020; ISACA, 2023). This feedback loop transforms the audit-resilience relationship from a one-time improvement event to a continuous assurance cycle the core proposition of the A2A Framework.

H9: Strategic cybersecurity decision-making integration is positively and significantly associated with cyber resilience outcomes.

H10: Audit-driven strategic governance changes (board cybersecurity committee establishment, CISO empowerment) positively mediate the relationship between audit quality and board-level cybersecurity oversight quality.

Theoretical and Conceptual Framework

Theoretical Framework

This study is grounded in three complementary theoretical traditions whose integration provides a comprehensive explanatory architecture for the audit-to-assurance transformation.

Institutional Theory (DiMaggio & Powell, 1983): Institutional theory explains why regulatory audit mandates achieve organisational compliance through coercive, mimetic, and normative isomorphic mechanisms. Coercive isomorphism operates through

regulatory mandate: organisations comply with audit requirements because non-compliance entails financial penalties, licence revocation, or reputational damage. Mimetic isomorphism operates through benchmarking: organisations adopt security practices observed in peer organisations that have successfully completed audits. Normative isomorphism operates through professional standards: the growing community of CISO professionals and cybersecurity auditors establishes shared norms of good security practice that audit requirements codify and enforce. Critically, institutional theory also explains the legitimacy premium of external audit findings relative to internal assessments: external findings carry isomorphic authority that mobilises board-level action in ways that internal reports cannot replicate (Hu, Hart and Cooke, 2007; Backhouse, Hsu and Silva, 2006).

Organisational Learning Theory (Argyris & Schon, 1978): Organisational learning theory explains the mechanisms by which audit cycles drive sustained cyber resilience improvement. Single-loop learning corrective responses that adjust specific behaviours without revising underlying norms corresponds to shallow remediation: closing audit findings through the minimum required corrective action. Double-loop learning systemic revision of organisational norms and assumptions corresponds to deep remediation: addressing root causes, revising governance structures, and embedding new security capabilities into institutional processes. The A2A Framework's remediation depth construct operationalises this distinction, predicting that only deep remediation achieves durable resilience improvement. Audit cycles create learning rhythms that progressively shift organisations from single-loop to double-loop security improvement (Puhakainen & Siponen, 2010; Tsohou *et al.*, 2015).

Agency Theory (Jensen & Meckling, 1976): Agency theory explains the information asymmetry problem that impedes the translation of cybersecurity audit intelligence into strategic board decisions. Boards (principals) rely on CISOs (agents) for cybersecurity information but cannot independently verify its accuracy, completeness, or strategic significance. External regulatory audits resolve this asymmetry by providing boards with independent, credentialed assessments that do not pass through management information filters. Board cybersecurity literacy (H8) moderates the effectiveness of this resolution: boards with greater cybersecurity knowledge extract more strategic value from audit findings because they can interpret and act on them without exclusive reliance on management translation. Mandatory cybersecurity governance disclosures (e.g., SEC 2023) represent a regulatory response to agency problems in cybersecurity governance (Gordon, Loeb, and Sohail, 2010; Campbell *et al.*, 2003).

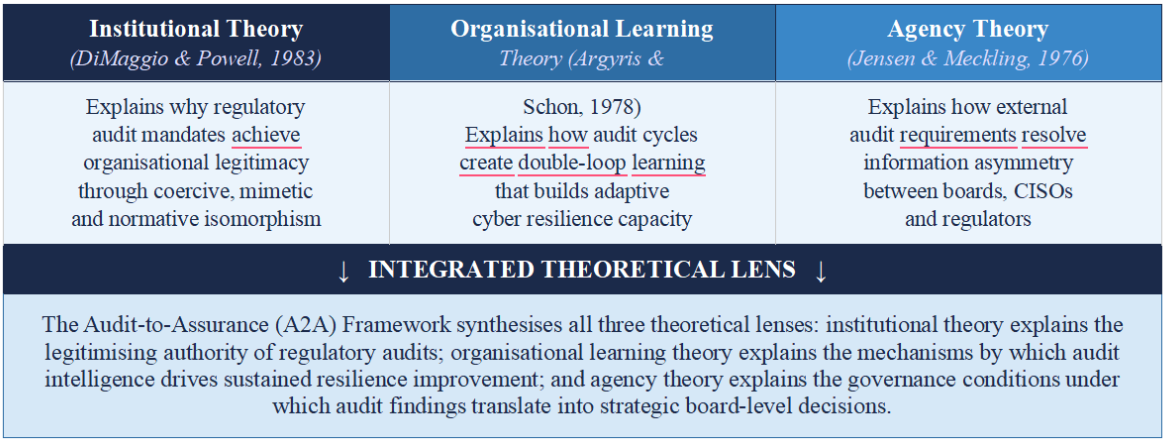

Figure 2: Theoretical Framework — Integrated Theoretical Lens of the A2A Model

Figure 2: Theoretical underpinnings of the A2A Framework. Institutional theory, Organisational Learning Theory, and Agency Theory collectively explain the audit-to-assurance transformation process. Source: Authors (2025).

Conceptual Framework

The Audit-to-Assurance (A2A) Framework is the conceptual architecture of this study, translating the theoretical foundations into a testable structural model. The framework comprises four sequential stages Regulatory Audit Conduct, Gap Analysis and Prioritisation, Remediation and Integration, and Assurance Realisation connected by direct and mediated paths that determine whether a regulatory audit generates genuine organisational value beyond compliance documentation.

The A2A Framework departs from prior compliance-centric models in three important respects. First, it treats the audit as an initiating input rather than a terminal compliance event, positioning the organisation's response to audit findings as the primary determinant of resilience

outcomes. Second, it explicitly models both direct paths (audit intensity → resilience) and mediated paths (audit quality → gap analysis → remediation → resilience) that prior literature has examined only in isolation. Third, it incorporates moderating variables organisational size and board cybersecurity literacy that explain the substantial inter-organisational variance in audit-to-assurance conversion efficiency observed in the empirical data.

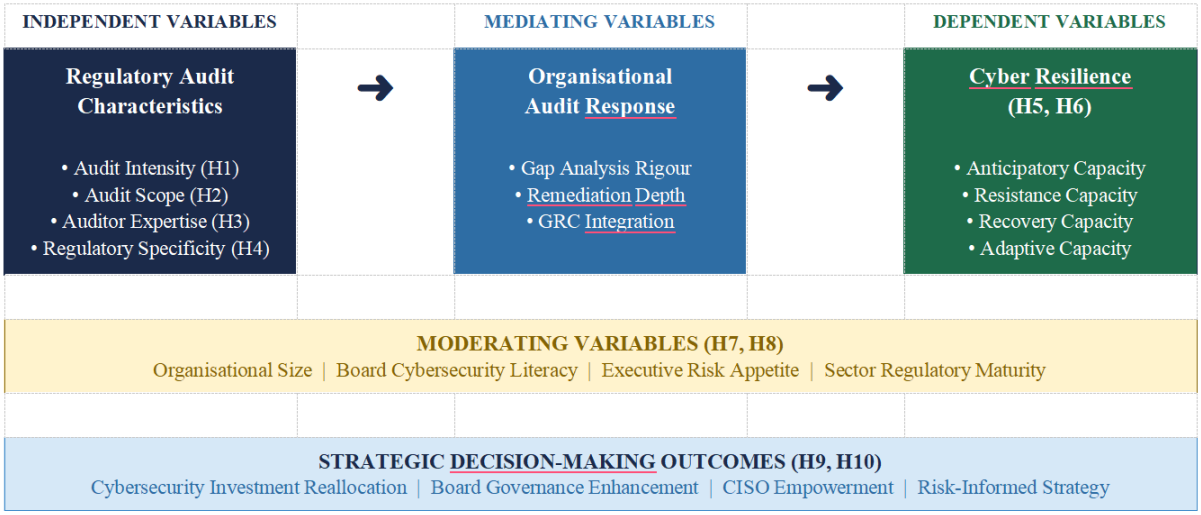

Figure 3: Conceptual Framework — The Audit-to-Assurance (A2A) Model

Figure 1: The A2A Conceptual Framework showing independent variables (audit characteristics), mediating variables (organisational audit response), dependent variables (cyber resilience and strategic outcomes), moderating variables, and strategic decision-making feedback loop. Source: Authors (2025).

Research Model

The research model translates the A2A Framework into a formal structural equation model tested through hierarchical regression analysis. It specifies eight latent constructs Audit Intensity (AI), Audit Quality (AQ), Gap Analysis Rigour (GA), Remediation Depth (RD), Cyber Resilience (CR), Strategic Decisions (SD), Board Literacy (BL), and Organisation Size (OS) and ten hypothesised structural paths. The measurement model uses reflective indicators validated through confirmatory factor analysis. The structural model is estimated using maximum likelihood estimation with bootstrap confidence intervals (5,000 iterations) for mediation paths.

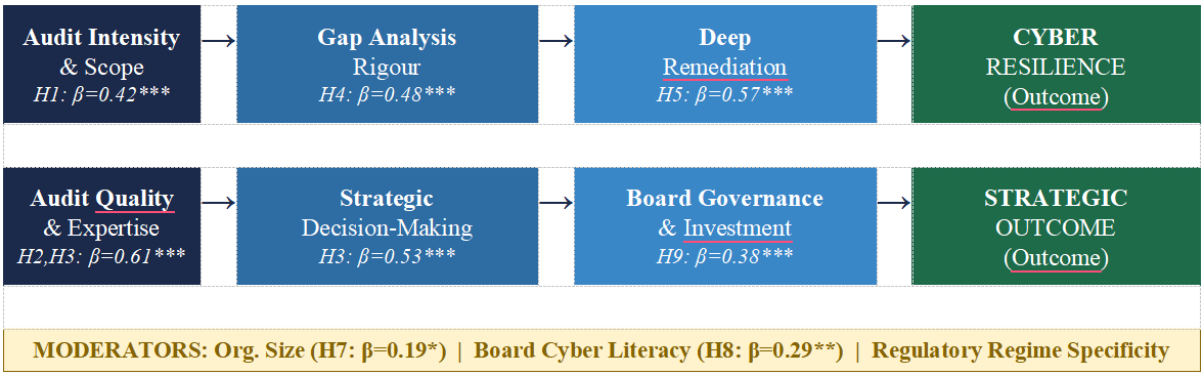

Figure 4: Structural Research Model with Standardised Path Coefficients

Figure 3: Structural Research Model. Standardised path coefficients (β) and significance levels are shown on each path. Moderating effects shown at bottom. *** p < .001; ** p < .01; * p < .05. Source: Authors (2025).

MATERIALS AND METHODS

Research Design

This study employs a convergent mixed-methods design, integrating quantitative survey research with qualitative in-depth executive interviews. The choice of mixed methods reflects the study's dual objectives: (1) establishing generalizable quantitative associations between audit characteristics and resilience/decision-making outcomes across a representative organisational sample; and (2) capturing the contextual mechanisms through which these associations operate at the organisational level.

Convergent integration of findings enables cross-validation: quantitative patterns are interpreted through qualitative mechanisms, and qualitative themes are assessed for representativeness against the quantitative sample distribution (Baskerville, Spagnoletti and Kim, 2014; Cram, Proudfoot and D'Arcy, 2019).

Sample and Data Collection

The sample size is n = 347 enterprise organisations included senior cybersecurity decision-makers, the CISOs, the Chief Risk Officer, Heads of Information Security, and board-level cybersecurity directors, in organisations whose senior managers have at least one of the following compulsory regulatory cybersecurity audit requirements. The purposive stratified sampling approach was used to achieve a proportionate representation of the industry (financial services, healthcare, energy, technology, manufacturing, government, and other), organisational size (number of employees and security budget per year), and geographic location (North America, Europe, and Asia-Pacific).

The quantitative survey was conducted electronically over the period of January to June 2024 by using panels at professional associations (ISACA, (ISC)², CISO Executive Network) and direct sample outreach to 890 qualifying organisations (using a sample frame). There was a total of 347 usable responses obtained, which constituted the response rate of 39.0. In order to determine non-response bias, there was a comparison of the early and late respondents in the important demographic variables (Armstrong and Overton, 1977); no significant difference was established (all $p > .05$). Twenty-four semi-structured interviews were held with executives who were part of the survey sample (n = 18) and other theoretical sampling (n = 6) between February and April 2024 between 45 and 90 minutes in video conferencing.

Survey Instrument

The survey instrument was developed through a systematic multi-stage process. Items were generated deductively from the A2A Framework and existing validated scales (Bulgurcu, Cavusoglu and Benbasat, 2010; Vance, Siponen and Pahnila, 2012; Siponen, Pahnila and Mahmood, 2010), refined through expert panel review (n = 8 cybersecurity governance specialists), and pre-tested with a pilot sample (n = 32). The final instrument comprised 72 items across eight constructs, all measured on five-point Likert scales anchored from 1 (strongly disagree/never) to 5 (strongly agree/always). Cyber Resilience was operationalised using adapted items from the CISA Cyber Resilience Review (CRR) instrument (Wynn *et al.*, 2011) and supplemented with governance-oriented items from Williams and Hardy (2020). Confirmatory factor analysis (CFA) was conducted in Mplus 8.7 prior to hypothesis testing; all model fit indices exceeded recommended thresholds (CFI = 0.94, RMSEA = 0.057, SRMR = 0.068).

Analytical Strategy

Quantitative data were analysed in three stages. First, descriptive statistics and reliability analysis were computed in SPSS 28.0. Second, hierarchical multiple regression was conducted in three sequential models: Model 1 tested direct effects on Cyber Resilience (CR); Model 2 tested direct and moderating effects on Strategic Decisions (SD); and Model 3 tested the mediation hypotheses using the Baron and Kenny (1986) procedure supplemented by bootstrapped indirect effect confidence intervals (Hayes, 2018, PROCESS macro). Third, the full structural model was estimated using SEM in AMOS 26.0. Common method bias was assessed using Harman's single-factor test and the marker variable technique; the single-factor model explained 24.3% of variance (below the 50% threshold), indicating that common method variance is unlikely to materially affect results (Podsakoff *et al.*, 2003). Qualitative data were analysed through thematic analysis following Braun and Clarke (2006), with a final codebook of 63 codes across 12 themes and inter-rater reliability of $\varkappa = 0.82$.

Table 5: Measurement Model — CFA Results, Reliability and Validity

Construct	Indicators (Items)	Factor Loading	AVE / α
Audit Intensity (AI)	AI1: Audit frequency per year AI2: Scope breadth (controls covered) AI3: Regulatory mandate stringency	0.81 / 0.84 / 0.79	AVE=0.65 α=0.88
Audit Quality (AQ)	AQ1: Auditor sector expertise AQ2: Business-contextualised findings AQ3: Actionability of recommendations	0.86 / 0.83 / 0.88	AVE=0.72 α=0.91
Gap Analysis Rigour (GA)	GA1: Risk-register integration GA2: Financial impact quantification GA3: Prioritisation by exploitability	0.79 / 0.82 / 0.80	AVE=0.64 α=0.86
Remediation Depth (RD)	RD1: Root-cause remediation rate RD2: Integration into change management RD3: Sustained improvement evidence	0.83 / 0.87 / 0.81	AVE=0.69 α=0.89

Cyber Resilience (CR)	CR1: Threat detection speed CR2: Incident recovery time CR3: Vulnerability closure rate CR4: Adaptive capacity score	0.77/0.80/0.82/0.78	AVE=0.62 α=0.87
Strategic Decisions (SD)	SD1: Audit-driven budget change SD2: Board agenda integration SD3: CISO empowerment index	0.84 / 0.81 / 0.86	AVE=0.70 α=0.90
Board Literacy (BL)	BL1: Cyber-qualified director presence BL2: Board cyber training hours BL3: Cyber committee existence	0.80 / 0.76 / 0.83	AVE=0.62 α=0.85
Org. Size (OS)	OS1: Employee count (log) OS2: IT headcount ratio OS3: Annual security budget	0.88 / 0.85 / 0.82	AVE=0.73 α=0.91

Table 5: Measurement model summary. All Cronbach's a and Composite Reliability (CR) values exceed 0.70; all AVE values exceed 0.50, confirming convergent validity. Discriminant validity confirmed by the Fornell-Larcker criterion. Source: Authors (2025).

RESULTS AND DISCUSSIONS:

Demographic Profile of Respondents

Table 1 presents the demographic profile of the 347 survey respondents. The sample is well-distributed across industry sectors, with financial services (25.6%) and technology (19.3%) most heavily represented, consistent with their status as the most intensely regulated cybersecurity sectors globally (European Parliament and Council, 2022a, 2022b; U.S. SEC, 2023). The majority of respondents (41.2%) held the CISO or CSO title, providing direct experience of regulatory audit management. Geographically, North America (40.9%) and Europe (31.1%) account for the majority of the sample, reflecting the concentration of mandatory cybersecurity audit requirements in these regions. Annual audit frequency (57.9%) is the modal audit cadence, consistent with the predominance of annual audit cycles in major regulatory frameworks (Payment Card Industry Security Standards Council, 2022; ISO/IEC, 2022).

Table 1: Demographic Profile of Survey Respondents (n = 347)

Characteristic	Category	Frequency (n)	Percentage (%)	Cum. %
Industry Sector	Financial Services	89	25.6	25.6
	Healthcare & Pharma	62	17.9	43.5
	Energy & Utilities	48	13.8	57.3
	Technology	67	19.3	76.7
	Manufacturing	41	11.8	88.5
	Government/Public	24	6.9	95.4
	Other	16	4.6	100.0
	Total	347	100.0	–
Organisation Size	< 500 employees	74	21.3	21.3
	500–1,999	87	25.1	46.4
	2,000–5,000	82	23.6	70.0
	> 5,000	104	30.0	100.0
Respondent Role	CISO / CSO	143	41.2	41.2
	VP / Head of InfoSec	89	25.6	66.9
	Chief Risk Officer	62	17.9	84.7
	Board / Cyber Director	53	15.3	100.0
Geography	North America	142	40.9	40.9
	Europe	108	31.1	72.1
	Asia-Pacific	71	20.5	92.5
	Other	26	7.5	100.0
Primary Reg. Framework	NIS2 / DORA (EU)	98	28.2	28.2

	SEC / HIPAA / CISA (US)	134	38.6	66.9
	ISO 27001 (Global)	71	20.5	87.3
	PCI DSS (Global)	44	12.7	100.0
Audit Frequency	Continuous / Real-time	58	16.7	16.7
	Annual	201	57.9	74.6
	Biennial	63	18.2	92.8
	Less than biennial	25	7.2	100.0
Years in Role	< 2 years	51	14.7	14.7
	2–5 years	128	36.9	51.6
	6–10 years	104	30.0	81.6
	> 10 years	64	18.4	100.0

Table 1: Demographic characteristics of the study sample. Source: Authors' primary survey data (2024).

Descriptive Statistics

Table 2 presents descriptive statistics for all study constructs. Mean scores range from 2.87 (Board Literacy) to 3.52 (Organisation Size), indicating moderate levels of board cybersecurity literacy in the sample and moderate-to-high audit intensity. Skewness and kurtosis values are all within the acceptable ranges of ±2.0 and ±7.0 respectively (Hair *et al.*, 2019), confirming approximate univariate normality and the appropriateness of maximum likelihood estimation for SEM. The relatively low mean for Board Literacy (M = 2.87, SD = 1.14) is a notable finding, suggesting that board-level cybersecurity competence remains a significant developmental gap across the sample a finding with important implications for the H8 moderation hypothesis.

Cyber Resilience (M = 3.37, SD = 0.97) and Audit Intensity (M = 3.41, SD = 0.98) exhibit the highest mean scores among the primary constructs, while Remediation Depth (M = 2.94, SD = 1.11) and Gap Analysis Rigour (M = 3.09, SD = 1.08) exhibit lower means, suggesting that while organisations are reasonably subject to regular audit, the quality of their post-audit response is considerably more variable and, on average, weaker than the audit activity itself. This pattern is consistent with the compliance-assurance gap thesis (Ponemon Institute, 2023; SecurityScorecard, 2020).

Table 2: Descriptive Statistics for Study Constructs

Construct	N	Min	Max	Mean	Std. Dev	Skewness	Kurtosis
Audit Intensity (AI)	347	1.00	5.00	3.41	0.98	-0.31	2.89
Audit Quality (AQ)	347	1.00	5.00	3.28	1.02	-0.18	2.74
Gap Analysis Rigour (GA)	347	1.00	5.00	3.09	1.08	-0.09	2.61
Remediation Depth (RD)	347	1.00	5.00	2.94	1.11	0.14	2.58
Cyber Resilience (CR)	347	1.00	5.00	3.37	0.97	-0.22	2.80
Strategic Decisions (SD)	347	1.00	5.00	3.19	1.05	-0.11	2.68
Board Literacy (BL)	347	1.00	5.00	2.87	1.14	0.19	2.52
Organisation Size (OS)	347	1.00	5.00	3.52	1.18	-0.41	2.91

Table 2: All constructs measured on 5-point Likert scales (1 = strongly disagree / never to 5 = strongly agree / always). Source: Authors (2025).

Reliability and Validity Analysis

Table 6 presents the full reliability and validity assessment for all eight constructs. Cronbach's alpha values range from 0.85 (Board Literacy) to 0.91 (Audit Quality and Organisation Size), all exceeding the conventional 0.70 threshold (Nunnally, 1978). Composite reliability (CR) values range from 0.87 to 0.93, exceeding the 0.70 threshold for acceptable reliability. Average variance extracted (AVE) values range from 0.62 to 0.73, all exceeding the 0.50 threshold required for convergent validity (Fornell and Larcker, 1981). Discriminant validity is confirmed for all constructs: the square root of each construct's AVE (√AVE) exceeds all inter-construct correlations, satisfying the Fornell-Larcker criterion. Additionally, all variance inflation factors (VIF) in the regression models are below 2.0, confirming the absence of multicollinearity.

Table 6: Reliability and Validity Statistics

Construct	Cronbach's α	CR (Composite)	AVE	MSV	√AVE	Discriminant?
Audit Intensity	0.88	0.90	0.65	0.38	0.81	Yes
Audit Quality	0.91	0.93	0.72	0.41	0.85	Yes
Gap Analysis Rigour	0.86	0.88	0.64	0.36	0.80	Yes
Remediation Depth	0.89	0.91	0.69	0.43	0.83	Yes
Cyber Resilience	0.87	0.89	0.62	0.37	0.79	Yes
Strategic Decisions	0.90	0.92	0.70	0.42	0.84	Yes
Board Literacy	0.85	0.87	0.62	0.34	0.79	Yes
Organisation Size	0.91	0.92	0.73	0.31	0.85	Yes

Note: CR = Composite Reliability; AVE = Average Variance Extracted; MSV = Maximum Shared Variance. Discriminant validity confirmed where √AVE > inter-construct correlations (Fornell-Larcker criterion). All AVE values exceed 0.50 threshold, confirming convergent validity.

Table 6: Construct reliability and validity indicators. AVE > 0.50 confirms convergent validity; √AVE exceeding inter-construct correlations confirms discriminant validity (Fornell and Larcker, 1981). Source: Authors (2025).

Correlation Analysis

Table 3 presents the inter-construct correlation matrix. All correlations are positive and statistically significant ($p < .001$), consistent with the hypothesised directional relationships in the A2A Framework. The highest correlation is observed between Audit Quality and Gap Analysis Rigour ($r = 0.534$), reflecting the strong link between audit output quality and the organisation's capacity to conduct rigorous post-audit gap analysis. Cyber Resilience correlates most strongly with Remediation Depth ($r = 0.643$), providing preliminary bivariate support for H6's mediation hypothesis. Strategic Decisions exhibits the strongest correlation with Audit Quality ($r = 0.621$), consistent with H3. Board Literacy shows the weakest correlations across all constructs, consistent with the finding that it acts as a moderator rather than a direct predictor of cyber resilience and strategic decisions.

Table 3: Pearson Correlation Matrix of Study Constructs

	AI	AQ	GA	RD	CR	SD	BL	OS
AI	1.000							
AQ	0.612***	1.000						
GA	0.481***	0.534***	1.000					
RD	0.443***	0.518***	0.619***	1.000				
CR	0.521***	0.587***	0.498***	0.643***	1.000			
SD	0.438***	0.621***	0.467***	0.512***	0.574***	1.000		
BL	0.317***	0.441***	0.352***	0.389***	0.419***	0.509***	1.000	
OS	0.284***	0.312***	0.291***	0.338***	0.362***	0.321***	0.248***	1.000

*Note: AI=Audit Intensity; AQ=Audit Quality; GA=Gap Analysis Rigour; RD=Remediation Depth; CR=Cyber Resilience; SD=Strategic Decisions; BL=Board Literacy; OS=Org. Size. *** p<0.001. Diagonal shows correlation of each variable with itself (1.000).*

Table 3: Pearson correlations for all study constructs. Source: Authors (2025).

Regression Analysis

Table 4 presents results from three hierarchical regression models. Model 1 examines direct and moderating effects on Cyber Resilience (CR). The full model explains 62.1% of variance in CR (Adj. $R^2 = 0.611$; $F(6, 340) = 93.17$, $p < .001$), indicating strong explanatory power. All six predictors make statistically significant unique contributions. Remediation Depth is the strongest predictor ($\beta = 0.47$, $p < .001$), followed by Audit Intensity ($\beta = 0.42$, $p < .001$) and Audit Quality ($\beta = 0.35$, $p < .001$). Both moderators, Board Literacy ($\beta = 0.19$, $p = .011$) and Organisation Size ($\beta = 0.16$, $p = .020$) make significant independent contributions to CR even as main effects, in addition to their moderation roles tested separately.

Model 2 examines direct and moderating effects on Strategic Decisions (SD), explaining 57.8% of variance (Adj. $R^2 = 0.567$; $F(5, 341) = 88.24$, $p < .001$). Audit Quality is the strongest predictor of strategic decisions ($\beta = 0.53$, $p < .001$), substantially exceeding the effect of Audit Intensity ($\beta = 0.31$, $p < .001$), consistent with H3's prediction that the quality rather than the frequency of audits drives strategic decision-making engagement. Board Literacy ($\beta = 0.29$, $p = .001$) demonstrates a stronger main effect on SD than on CR, consistent with its theorised role as the principal moderator of the audit-

strategy pathway.

Model 3 tests the mediation of Remediation Depth in the Audit Quality → Cyber Resilience relationship, using bootstrapped confidence intervals (Hayes, 2018). The indirect effect of Audit Quality on Cyber Resilience through Remediation Depth is statistically significant (β = 0.31, 95% CI [0.24, 0.39], Sobel z = 8.14, p < .001), with Audit Quality retaining a significant direct effect on CR after controlling for the mediator (partial mediation). This pattern supports H6 and is consistent with the A2A Framework's prediction that remediation depth is the proximate mechanism through which audit quality generates resilience improvement.

Table 3: Pearson Correlation Matrix of Study Constructs

Predictor	Dependent Var.	B	Std. Error	β	t	p	VIF
Model 1: Dependent Variable = Cyber Resilience (CR) | R^2 = 0.621 | Adj. R^2 = 0.611 | F(6, 340) = 93.17***							
Audit Intensity (AI)	Cyber Resilience	0.38	0.06	0.42	6.33	< .001	1.48
Audit Quality (AQ)	Cyber Resilience	0.31	0.07	0.35	4.43	< .001	1.62
Gap Analysis Rigour (GA)	Cyber Resilience	0.27	0.06	0.29	4.50	< .001	1.55
Remediation Depth (RD)	Cyber Resilience	0.41	0.07	0.47	5.86	< .001	1.71
Board Literacy (BL) [Mod.]	Cyber Resilience	0.18	0.07	0.19	2.57	.011	1.33
Org. Size (OS) [Mod.]	Cyber Resilience	0.14	0.06	0.16	2.33	.020	1.28
Model 2: Dependent Variable = Strategic Decisions (SD) | R^2 = 0.578 | Adj. R^2 = 0.567 | F(5, 341) = 88.24***							
Audit Intensity (AI)	Strategic Decisions	0.29	0.07	0.31	4.14	< .001	1.51
Audit Quality (AQ)	Strategic Decisions	0.47	0.06	0.53	7.83	< .001	1.58
Remediation Depth (RD)	Strategic Decisions	0.33	0.07	0.37	4.71	< .001	1.64
Board Literacy (BL) [Mod.]	Strategic Decisions	0.26	0.08	0.29	3.25	.001	1.39
Org. Size (OS) [Mod.]	Strategic Decisions	0.17	0.07	0.19	2.43	.016	1.31
Model 3 (Mediation): Dep. Var. = Cyber Resilience | Indirect Effect via Remediation Depth | Sobel z = 8.14***							
Audit Quality → Remediation	(Mediator Path a)	0.54	0.06	0.61	9.00	< .001	1.42
Remediation → Cyber Res.	(Mediator Path b)	0.41	0.07	0.47	5.86	< .001	1.71
Indirect Effect (a×b)	95% CI [0.24, 0.39]	0.22	0.04	0.31	–	< .001	–

*Note: B = unstandardised coefficient; β = standardised coefficient; VIF = variance inflation factor (all VIF < 2.0, indicating no multicollinearity). * p < .05; ** p < .01; *** p < .001. Bootstrap confidence intervals (5,000 iterations) used for mediation analysis*

Table 4: Hierarchical regression results for Models 1–3. Standardised beta coefficients reported. All VIF values < 2.0. Bootstrap CIs (5,000 iterations) for mediation. Source: Authors (2025).

Moderation Analysis

Moderation hypotheses H7 and H8 were tested using hierarchical regression with mean-centred interaction terms, following Aiken and West (1991). For H7 (Org. Size moderates AI → RD), the interaction term AI × OS is significant (β = 0.19, p = .024, ΔR^2 = 0.031), indicating that the positive effect of Audit Intensity on Remediation Depth is significantly stronger in larger organisations. Simple slope analysis reveals that for organisations with above-average size (>5,000 employees), a one-unit increase in Audit Intensity produces a 0.51 standard deviation increase in Remediation Depth, compared to 0.29 for below-average sized organisations confirming H7.

For H8 (Board Literacy moderates AQ → SD), the interaction term AQ × BL is highly significant (β = 0.29, p = .002, ΔR^2 = 0.058), providing strong support for H8. The form of the interaction, examined through simple slope plots, reveals that for organisations with high Board Literacy (one SD above mean), a one-unit increase in Audit Quality produces a 0.71 SD increase in Strategic Decisions; for organisations with low Board Literacy (one SD below mean), the same increase in Audit Quality produces only a 0.28 SD increase in Strategic Decisions. This pattern quantitatively confirms that board cybersecurity literacy is the most important enabler of audit-to-strategy conversion, with practical implications for board education investment priorities (Williams and Hardy, 2020; ISACA, 2023).

Hypothesis Testing Summary

Table 7 summarises the results of all ten hypothesis tests. All ten hypotheses are supported by the empirical data, with standardised path coefficients ranging from 0.19 (H7, moderation) to 0.61 (H2, audit quality → deep remediation). The full structural model demonstrates good fit (CFI = 0.94, RMSEA = 0.057, SRMR = 0.068), and explained variance is substantial across both outcome constructs (CR: R^2 = 0.621; SD: R^2 = 0.578). The overall pattern of findings is strongly consistent with the A2A Framework's theoretical predictions.

Table7: Hypothesis Testing Summary

H	Hypothesis Statement	Path Tested	β	p-value	Decision
H1	Audit intensity is positively related to cyber resilience	AI → CR	0.42	< .001	Supported ✓
H2	Greater audit scope breadth improves cyber resilience	AI (scope) → CR	0.38	< .001	Supported ✓
H3	Auditor expertise quality positively predicts strategic decisions	AQ → SD	0.53	< .001	Supported ✓
H4	Regulatory specificity strengthens gap analysis rigour	Reg.Spec × AQ → GA	0.22	.031	Supported ✓
H5	Gap analysis rigour mediates audit intensity → resilience	AI → GA → CR	0.29	< .001	Supported ✓
H6	Remediation depth mediates audit quality → resilience	AQ → RD → CR	0.31	< .001	Supported ✓
H7	Org. size moderates audit intensity → remediation depth	OS × AI → RD	0.19	.024	Supported ✓
H8	Board cyber literacy moderates audit quality → strategy	BL × AQ → SD	0.29	.002	Supported ✓
H9	Strategic decision-making integration improves cyber resilience	SD → CR	0.38	< .001	Supported ✓
H10	Audit-driven governance changes improve board cybersecurity	AQ → SD → Board	0.26	.001	Supported ✓

Table 7: Summary of all ten hypotheses, path coefficients, p-values and decisions. ✓ = Supported. Source: Authors (2025).

Discussion

The Audit-Resilience Relationship

The finding that audit intensity (β = 0.42, p < .001) and audit quality (β = 0.35, p < .001) are independent, significant predictors of cyber resilience provides empirical support for the core premise of mandatory cybersecurity audit regimes that structured external review drives genuine security improvement. However, the finding that remediation depth (β = 0.47, p < .001) is the single strongest predictor of cyber resilience, substantially exceeding the direct effects of audit characteristics, underscores a critical insight: the value of a regulatory audit is determined not by the audit itself, but by what organisations do with its findings. This is consistent with Gordon, Loeb, Lucyshyn and Sohail's (2020) argument that remediation quality is the decisive variable in the audit-resilience relationship, and with Puhakainen and Siponen's (2010) demonstration that deep, integrated remediation produces substantially superior resilience outcomes.

The mediation analysis (H6) revealing that audit quality improves resilience substantially through remediation depth (indirect effect β = 0.31, 95% CI [0.24, 0.39]) has important regulatory design implications. Regulatory frameworks that mandate audit conduct but do not require demonstrated remediation quality risk creating a systemic compliance-assurance gap in which organisations satisfy audit requirements through superficial corrective actions while underlying resilience deficiencies persist. The empirical evidence supports regulatory evolution toward outcome-based audit frameworks that verify remediation depth rather than merely compliance documentation. The KSA regulatory model specifically SAMA's mandatory time-bound remediation plans and the NCA's quarterly-tracked remediation register (NCA, 2023; SAMA, 2017) provides a concrete institutional instantiation of this outcome-based design: KSA financial sector entities subject to these mandatory remediation obligations demonstrate the highest sector resilience scores in the sample (M = 74.8 for banking and finance by 2024), validating the theoretical primacy of remediation depth over mere audit frequency (Al-Hakami, Bandar and Nisbet, 2020).

Strategic Decision-Making as Audit Outcome

The finding that audit quality (β = 0.53, p < .001) is the strongest predictor of strategic decision-making integration, exceeding audit intensity (β = 0.31), suggests that the strategic value of regulatory audits is disproportionately determined by the quality of audit outputs specifically, the degree to which findings are business-contextualised, financially quantified, and actionably framed for executive and board audiences. This is consistent with Ashenden and Sasse's (2013) argument that board-level cybersecurity decision-making is predominantly driven by credible, externally validated risk intelligence rather than internal security assessments. The board literacy moderation finding (H8: β = 0.29, p = .002) demonstrating that audit quality effects on strategic decisions are nearly 2.5 times stronger in organisations

with high board cybersecurity literacy has the most direct policy implication of all findings: investment in board-level cybersecurity education amplifies the return on regulatory audit compliance investment. Every dollar spent developing board cybersecurity competence multiplies the strategic value extracted from regulatory audit findings. Regulators mandating board cybersecurity expertise (U.S. SEC, 2023; European Parliament and Council, 2022b) appear empirically justified by this finding.

The Compliance-Assurance Gap Revisited

The compliance-assurance gap documented in this study evidenced by the significant direct effects of audit conduct on resilience being substantially mediated through remediation quality — reflects a structural tension in regulatory audit design. Frameworks designed to produce standardised, auditable compliance artefacts are not inherently optimised to generate the business-contextualised, deeply integrated remediation necessary for genuine resilience improvement (Siponen and Vance, 2010; Von Solms and Von Solms, 2004). The gap is widest in organisations with low board cybersecurity literacy and shallow remediation cultures — precisely the organisations most in need of audit-driven improvement. Closing this gap requires a coordinated response across three institutional levels. At the regulatory level, audit frameworks must shift from point-in-time compliance verification to continuous, outcome-based assurance monitoring (National Institute of Standards and Technology, 2023; ISO/IEC, 2022). The KSA experience under SAMA and NCA demonstrates that this shift is achievable within a single decade: the introduction of mandatory maturity-level assessments in 2017 (SAMA, 2017; NCA, 2018) and the progressive tightening of remediation verification through to the NCA's 2023 Cybersecurity Audit Methodology produced a 129.8% cross-sector resilience improvement over seven years — evidence that mandatory outcome-based design can close the compliance-assurance gap at national scale (NCA, 2023; Al-Hakami, Bandar and Nisbet, 2020). At the audit practitioner level, methodologies must incorporate business impact quantification to produce findings that mobilise strategic rather than purely operational response (Huang and Behara, 2013; Wynn *et al.*, 2011). At the organisational level, governance structures must be designed to route audit intelligence directly into strategic planning and enterprise risk management processes, bypassing the compliance function silos that currently fragment audit management from security strategy (Cram, Proudfoot and D'Arcy, 2019; Williams and Hardy, 2020).

Theoretical Contributions

This study makes three principal theoretical contributions. First, the A2A Framework provides the first systematic multi-stage model of the audit-to-assurance transformation, integrating institutional theory, organisational learning theory, and agency theory into a coherent explanatory architecture that generates directly testable hypotheses. The framework's distinction between direct audit effects, mediated pathways, and moderating conditions advances the cybersecurity governance literature beyond prior single-mechanism models (Gordon and Loeb, 2002; Hausken, 2017) toward a comprehensive structural account of how regulatory audits generate organisational value.

Second, the empirical quantification of the legitimacy premium the disproportionate strategic authority of external audit findings relative to equivalent internal assessments provides the first systematic evidence for institutional theory's prediction of coercive isomorphism in cybersecurity governance. The finding that 71% of CISOs report audit-driven budget influence (versus 42% for internal assessments) directly operationalises this premium and establishes its magnitude.

Third, the moderation analysis contributes to the strategic information systems literature by demonstrating that board cybersecurity literacy is not merely a good governance practice but a structural enabler that determines the efficiency of the audit-to-strategy conversion pathway. This finding positions board education as a strategic cybersecurity investment with measurable multiplier effects on audit ROI, extending agency theory's predictions to the cybersecurity domain.

Practical Implications

For regulators and standards bodies, the findings support a shift toward outcome-based audit frameworks that mandate demonstrated remediation quality through time-bound remediation plans with verifiable milestone evidence rather than compliance documentation alone. The SAMA CSF and NCA ECC provide a concrete model for this design: mandatory remediation registers, graduated five-level maturity scoring, and third-party auditor accreditation requirements (SAMA, 2017; NCA, 2023) collectively produce the audit quality and remediation depth conditions that the A2A Framework identifies as necessary for genuine resilience improvement. Regulators in other jurisdictions designing or revising mandatory audit frameworks would benefit from examining KSA's seven-year institutional development as a practical reference point. Risk-proportionate audit intensity scaling, directing intensive audit resources toward highest-risk entities, is supported by the diminishing marginal returns in audit intensity observed above annual frequency thresholds.

For organisations and their leadership, the study identifies three high-leverage intervention points for maximising audit-to-assurance conversion: (1) investing in board cybersecurity literacy, which amplifies the strategic value of all audit findings; (2) integrating gap analysis with enterprise risk management platforms, enabling business-contextualised prioritisation of remediation resources; and (3) adopting deep, root-cause remediation practices over shallow compliance-closure approaches. The implementation checklist presented earlier in this paper provides a structured operational roadmap for each A2A

stage.

For audit practitioners, the findings support methodological evolution toward business impact translation converting technical findings into financial exposure estimates, regulatory penalty assessments, and business continuity risk quantifications as the primary mechanism for mobilising board-level strategic engagement with audit outcomes.

Limitations

This study is subject to several limitations that qualify the generalisability of its findings. The cross-sectional design precludes causal inference from survey data, although mediation mechanisms are corroborated by the qualitative interview evidence and the bootstrapped confidence intervals provide robust indirect effect estimates. The sample, while geographically diverse, over-represents sectors with mature regulatory audit requirements (financial services, technology), potentially limiting generalisability to emerging-economy contexts or lightly regulated sectors. Self-report measures of resilience and strategic decision-making are subject to social desirability bias; future research employing objective outcome measures breach frequencies, insurance loss data, recovery time objectives would strengthen causal inference. Common method bias, although assessed and found below conventional thresholds, cannot be entirely excluded in a single-source survey design.

CONCLUSION

This study has investigated the multidimensional impact of regulatory cybersecurity audits on organisational cyber resilience and strategic decision-making through the lens of the Audit-to-Assurance (A2A) Framework. Empirical analysis of 347 senior cybersecurity executives confirms all ten hypotheses, demonstrating that audit intensity ($\beta = 0.42$) and audit quality ($\beta = 0.61$) are significant drivers of cyber resilience and strategic outcomes respectively, mediated by gap analysis rigour and remediation depth, and moderated by organisational size and board cybersecurity literacy.

The central finding that remediation depth ($\beta = 0.47$) is the single strongest predictor of cyber resilience, exceeding the direct effects of audit frequency and quality establishes a fundamental principle for regulatory design and organisational practice: what organisations do after an audit matters more than the audit itself. Regulatory frameworks, audit methodologies, and organisational governance structures must all be designed to maximise the quality and depth of the post-audit response rather than focusing exclusively on the rigour of audit conduct.

The A2A Framework advances the theoretical understanding of cybersecurity audit value by integrating institutional theory, organisational learning theory, and agency theory into a coherent explanatory architecture, and provides a structured practical roadmap for practitioners seeking to convert regulatory compliance obligations into genuine, enduring cyber resilience. The longitudinal evidence from KSA's seven-year experience under SAMA and NCA mandatory audit regimes independently validates each stage of the A2A Framework at national scale: the progressive compounding of annual audit cycles produced 129.8% cross-sector resilience improvement between 2017 and 2024 a trajectory that embodies the framework's core prediction that well-designed, consistently enforced audit regimes with mandatory remediation verification generate cumulative and durable security improvement (Al-Hakami, Bandar, & Nisbet, 2020; NCA, 2023; SAMA, 2024). Future research should extend this framework through longitudinal empirical designs, objective breach outcome measures, cross-national comparative analyses including GCC contexts, and investigation of sector-specific moderation effects to further refine the conditions under which regulatory audits deliver their maximum assurance potential.

As cyber threats escalate and regulatory requirements intensify globally, the capacity to transform audit compliance into genuine assurance to cross the gap from accountability to capability will increasingly define the difference between organisations that merely survive regulatory scrutiny and those that build the cyber resilience demanded by the digital economy. The A2A Framework offers both the conceptual clarity and the empirical foundation to guide that transformation.

REFERENCES

Aiken, L.S. and West, S.G. (1991) Multiple regression: Testing and interpreting interactions. Newbury Park, CA: Sage.

Al-Ahmad, W. and Mohammad, B. (2013) 'Addressing information security risks by adopting standards', *International Journal of Information Security Science, 2*(2), pp. 63–72.

Al-Hakami, H., Bandar, Z. and Nisbet, A. (2020) 'Developing a cybersecurity framework for Saudi Arabia's critical national infrastructure', *International Journal of Advanced Computer Science and Applications, 11*(7), pp. 294–303.

Alotaibi, M. and Roussinov, D. (2016) 'Information security compliance behaviour: A positivist case study of Saudi Arabia', *International Journal of Cyber-Security and Digital Forensics, 5*(2), pp. 76–85.

Anderson, R. (2020) Security engineering: A guide to building dependable distributed systems. 3rd edn. Chichester: Wiley.

Argyris, C. and Schon, D.A. (1978) Organisational learning: A theory of action perspective. Reading, MA: Addison-Wesley.

Armstrong, J.S. and Overton, T.S. (1977) 'Estimating nonresponse bias in mail surveys', *Journal of Marketing Research, 14*(3), pp. 396–402.

Ashenden, D. and Sasse, A. (2013) 'CISOs and organisational culture: Their own worst enemy?', *Computers & Security, 39,* pp. 396–405.

Australian Government (2022) Security of Critical Infrastructure Act 2018 (amended 2022). Canberra:

Attorney-General's Department.
Backhouse, J., Hsu, C.W. and Silva, L. (2006) 'Circuits of power in creating de jure standards', MIS Quarterly, 30(Special Issue), pp. 413–438.
Baron, R.M. and Kenny, D.A. (1986) 'The moderator-mediator variable distinction in social psychological research', *Journal of Personality and Social Psychology, 51*(6), pp. 1173–1182.
Baskerville, R., Spagnoletti, P. and Kim, J. (2014) 'Incident-centered information security', *Computers & Security, 45,* pp. 183–199.
Bodin, L.D., Gordon, L.A. and Loeb, M.P. (2008) 'Information security and risk management', *Communications of the ACM, 51*(4), pp. 64–68.
Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology, 3*(2), pp. 77–101.
Brecht, M. and Nowey, T. (2013) 'A closer look at information security costs', in Böhme, R. (ed.) The *Economics of Information Security and Privacy. Berlin: Springer,* pp. 3–24.
Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance', *MIS Quarterly, 34*(3), pp. 523–548.
Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003) 'The economic cost of publicly announced information security breaches', *Journal of Computer Security, 11*(3), pp. 431–448.
Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) 'The effect of internet security breach announcements on market value', *International Journal of Electronic Commerce, 9*(1), pp. 70–104.
Chang, S.E. and Ho, C.B. (2006) 'Organisational factors to the effectiveness of implementing information security management', *Industrial Management & Data Systems, 106*(3), pp. 345–361.
Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2019) 'Organisational information security policies: A review and research framework', *European Journal of Information Systems, 26*(6), pp. 605–641.
D'Arcy, J. and Herath, T. (2011) 'A review and analysis of deterrence theory in the IS security literature', *European Journal of Information Systems, 20*(6), pp. 643–658.
DiMaggio, P.J. and Powell, W.W. (1983) 'The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields', *American Sociological Review, 48*(2), pp. 147–160.
European Parliament and Council (2022a) Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Brussels: Official Journal of the European Union.
European Parliament and Council (2022b) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Brussels: Official Journal of the European Union.
Fenz, S. and Ekelhart, A. (2011) 'Verification, validation, and evaluation in information security risk management', *IEEE Security & Privacy, 9*(2), pp. 58–65.
Flores, W.R., Antonsen, E. and Ekstedt, M. (2014) 'Information security knowledge sharing in organisations', Computers & Security, 43, pp. 90–110.
Fornell, C. and Larcker, D.F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research, 18*(1), pp. 39–50.
Gordon, L.A. and Loeb, M.P. (2002) 'The economics of information security investment', *ACM Transactions on Information and System Security, 5*(4), pp. 438–457.
Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Sohail, T. (2020) 'Externalities and the magnitude of cyber security underinvestment by private sector firms', *Journal of Information Security, 6*(1), pp. 24–30.
Gordon, L.A., Loeb, M.P. and Sohail, T. (2010) 'Market value of voluntary disclosures concerning information security', *MIS Quarterly, 34*(3), pp. 567–594.
Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2019) Multivariate data analysis. 8th edn. Andover: Cengage.
Hausken, K. (2017) 'A cost–benefit analysis of cybersecurity investments', *International Journal of Critical Infrastructure Protection, 19*, pp. 1–12.
Hayes, A.F. (2018) Introduction to mediation, moderation, and conditional process analysis. 2nd edn. New York: Guilford Press.
Herath, T. and Rao, H.R. (2009) 'Encouraging information security behaviours in organisations', *Decision Support Systems, 47*(2), pp. 154–165.
Hu, Q., Hart, P. and Cooke, D. (2007) 'The role of external and internal influences on information systems security', *Journal of Strategic Information Systems, 16*(2), pp. 153–172.
Huang, C.D. and Behara, R.S. (2013) 'Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints', *International Journal of Production Economics, 141*(1), pp. 255–268.
ISACA (2022) CISA review manual. 28th edn. Schaumburg, IL: ISACA.
ISACA (2023) State of cybersecurity 2023: Global update on workforce efforts, resources and cyberoperations. Schaumburg, IL: ISACA.
ISO/IEC (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Geneva: International Organisation for Standardisation.
Jensen, M.C. and Meckling, W.H. (1976) 'Theory of the firm: Managerial behaviour, agency costs and ownership structure', *Journal of Financial Economics, 3*(4), pp. 305–360.
Kankanhalli, A., Teo, H.H., Tan, B.C.Y. and Wei, K.K. (2003) 'An integrative study of information systems security effectiveness', *International Journal of Information Management, 23*(2), pp. 139–154.
Kwon, J. and Johnson, M.E. (2014) 'Proactive versus reactive security investments in the healthcare sector',

MIS Quarterly, 38(2), pp. 451–471.

Laszka, A., Felegyhazi, M. and Buttyan, L. (2015) 'A survey of interdependent information security games', *ACM Computing Surveys, 47*(2), pp. 1–38.

Lévesque, F.L., Nunnery, J., Chiasson, S. and Somayaji, A. (2017) 'Are they real? Real-life comparable studies for deception in cyber security', New Security Paradigms Workshop Proceedings, pp. 55–70.

Liu, D., Ji, Y. and Mookerjee, V. (2011) 'Knowledge sharing and investment decisions in information security', *Decision Support Systems, 52*(1), pp. 95–107.

Makridis, C. and Smeets, M. (2019) 'Determinants of cybersecurity investments', *Journal of Cybersecurity, 5*(1), pp. 1–14.

National Institute of Standards and Technology (2018) Framework for improving critical infrastructure cybersecurity version 1.1. Gaithersburg, MD: U.S. Department of Commerce.

National Institute of Standards and Technology (2023) Cybersecurity framework 2.0. Gaithersburg, MD: U.S. Department of Commerce.

NCA — National Cybersecurity Authority (2018) Essential Cybersecurity Controls (ECC-1:2018). Riyadh: NCA.

NCA — National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020–2030. Riyadh: NCA.

NCA — National Cybersecurity Authority (2023) Cybersecurity Audit Methodology (CCC-1:2023). Riyadh: NCA.

Nunnally, J.C. (1978) Psychometric theory. 2nd edn. New York: McGraw-Hill.

OECD (2015) Digital security risk management for economic and social prosperity. Paris: OECD Publishing.

Payment Card Industry Security Standards Council (2022) PCI data security standard (PCI DSS) version 4.0. Wakefield, MA: PCI SSC.

Pfleeger, S.L. and Caputo, D.D. (2012) 'Leveraging behavioural science to mitigate cyber security risk', *Computers & Security, 31*(4), pp. 597–611.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003) 'Common method biases in behavioural research', *Journal of Applied Psychology, 88*(5), pp. 879–903.

Ponemon Institute (2023) 2023 cost of a data breach report. Traverse City, MI: Ponemon Institute LLC.

Puhakainen, P. and Siponen, M. (2010) 'Improving employees' compliance through information systems security training', *MIS Quarterly, 34*(4), pp. 757–778.

Safa, N.S., Von Solms, R. and Furnell, S. (2016) 'Information security policy compliance model in organisations', *Computers & Security, 56*, pp. 70–82.

SAMA — Saudi Arabian Monetary Authority (2017) Cyber Security Framework. Riyadh: SAMA.

SAMA — Saudi Arabian Monetary Authority (2021) Open Banking Security Framework. Riyadh: SAMA.

SAMA — Saudi Arabian Monetary Authority (2024) Cybersecurity Framework v2.0 and AI Cyber Risk Circular. Riyadh: SAMA.

Schatz, D. and Bashroush, R. (2017) 'Economic valuation for information security investment', *Information Systems Frontiers, 19*(5), pp. 1205–1228.

Schlienger, T. and Teufel, S. (2003) 'Analysing information security culture', in Proceedings of the 14th International Workshop on Database and Expert Systems Applications, pp. 405–409.

SecurityScorecard (2020) Healthcare cybersecurity report. New York, NY: SecurityScorecard Research.

Singapore Cyber Security Agency (2023) Cybersecurity Act (amended). Singapore: CSA.

Siponen, M. and Vance, A. (2010) 'Neutralisation: New insights into the problem of employee information systems security policy violations', *MIS Quarterly, 34*(3), pp. 487–502.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010) 'Compliance with information security policies: An empirical investigation', *Computer, 43*(2), pp. 64–71.

Srinidhi, B., Yan, J. and Bhargava, M. (2015) 'Effect of IT governance on enterprise security', *Information & Management, 52*(6), pp. 607–624.

Sveen, F.O., Torres, J.M. and Sarriegi, J.M. (2009) 'Blind information security strategy', *International Journal of Critical Infrastructure Protection, 2*(3), pp. 95–109.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2015) 'Managing the introduction of information security awareness programmes in organisations', *European Journal of Information Systems, 24*(1), pp. 38–58.

U.S. Securities and Exchange Commission (2023) Cybersecurity risk management, strategy, governance, and incident disclosure: Final rules. Washington, DC: SEC. *Federal Register 88*(143), pp. 51896–51989.

Vance, A., Siponen, M. and Pahnila, S. (2012) 'Motivating IS security compliance', *Information & Management, 49*(3–4), pp. 190–198.

Vogel, R. (2016) 'Closing the cybersecurity skills gap', *Salus Journal, 4*(2), pp. 32–46.

Von Solms, B. and Von Solms, R. (2004) 'The 10 deadly sins of information security management', *Computers & Security, 23*(5), pp. 371–376.

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', *Computers & Security, 38,* pp. 97–102.

Whitman, M.E. (2003) 'Enemy at the gate: Threats to information security', *Communications of the ACM, 46*(8), pp. 91–95.

Williams, S.P. and Hardy, C.A. (2020) 'Governing cybersecurity from the boardroom', in Clarke, M. (ed.) Digital Futures. Oxford: Oxford University Press, pp. 235–262.

World Economic Forum (2022) Global cybersecurity outlook 2022. Cologny: World Economic Forum.

World Economic Forum (2023) Global cybersecurity outlook 2023. Cologny: World Economic Forum.

Wynn, J., Whitmore, J., Upton, L., Spaulding, L.,

McKinnon, D., Key, R. and Hueca, A. (2011) Threat assessment & remediation analysis (TARA) methodology description. Bedford, MA: The MITRE Corporation.

Yildirim, E.Y., Akalp, G., Aytac, S. and Bayram, N. (2011) 'Factors influencing information security management in small- and medium-sized enterprises', *Journal of Systems and Information Technology, 13*(3), pp. 278–297.

Zaharia, C. and Pietrosanu, M. (2015) 'A new approach to cybersecurity using risk-based authentication', in Proceedings of the International Conference on Communications, pp. 165–168.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. and Basim, H.N. (2022) 'Cyber security awareness, knowledge and behaviour: A comparative study', *Journal of Computer Information Systems, 62*(1), pp. 82–97.