Accounting, Auditing & Accountability Journal

Building public sector cyber-resilience through performance audit: responses to cybersecurity risks

Carolyn J. Cordery
School of Accounting and Commercial Law, Victoria University of Wellington, Wellington, New Zealand, and
Tarek Rana
Department of Accounting, RMIT University, Melbourne, Australia

Received 23 September 2025
Revised 8 March 2026
28 June 2026
Accepted 4 July 2026

Abstract

Purpose – This study asks which Performance Audit (PA) practices Supreme Audit Institutions (SAIs) prioritize to address cybersecurity risks and how these contribute to public sector cyber-resilience.

Design/methodology/approach – Drawing on semi-structured interviews with sector participants across several jurisdictions, complemented by documentary analysis and international training materials, our exploratory qualitative design analyses the reconfiguration of PA practices to respond to public sector cyber-resilience imperatives.

Findings – We show that public sector cyber-resilience goals re-temporalize and re-scale PA. Rather than focusing primarily on retrospective compliance, high-functioning SAIs increasingly orient PA towards anticipatory, system-level and future-facing forms of governance. Empirically, this shift is expressed through new audit objects, new audit practices and new audit products. Combined, these changes reposition PA as a catalytic and infrastructural governance device for building public sector cyber-resilience.

Research limitations/implications – PA contributes most strongly to cyber-resilience planning and anticipatory preparedness and increasingly to absorptive capacity, while recovery and adaptation remain uneven and often constrained by mandates, capabilities and institutional boundaries. Thus, PA has potential for, and limitations in, governing cybersecurity risk. The imperative of cyber-resilience underscores emerging tensions between independence, collaboration, transparency and security in cyber-related audits.

Originality/value – What is new here is not "audit adapts to cybersecurity risk", but that public sector cyber-resilience forces a reconfiguration of what counts as auditable, when audit intervenes (ex-ante or ex-post) and what the audit product is (including guidance, simulations, readiness reviews and cross-system coordination). Thus, PA moves beyond retrospective evaluation towards anticipatory and system-oriented governance.

Keywords Performance audit, Cyber-resilience, Cybersecurity, Risk management, Supreme audit institutions, Public sector

Paper type Research article

1. Introduction

Public sector organizations across advanced and emerging economies are undergoing rapid digital transformation, with core public services, infrastructures and regulatory functions increasingly dependent on complex, interconnected information systems (Sundberg and Holmström, 2024; Twizeyimana and Andersson, 2019). While digitalization promises efficiency, accessibility and new forms of public value creation, it simultaneously introduces systemic cybersecurity risk vulnerabilities, including ransomware attacks, data breaches and critical service disruptions (INTOSAI IDI Development Initiative, 2022). Recent high-profile incidents affecting hospitals, airports, tax authorities and social welfare systems have underscored that cyber threats are no longer peripheral technical issues but central governance

Accounting, Auditing & Accountability Journal
Emerald Publishing Limited
e-ISSN: 1758-4205
p-ISSN: 1368-0668
DOI 10.1108/AAAJ-09-2025-8354

risks with profound societal consequences (Gordon *et al*., 2008; Lehto and Limnéll, 2021; Wirtz and Weyerer, 2017). Thus, it is inadequate to conceive that cybersecurity requires merely compliance with technical standards that can be easily audited; rather, cyber-resilience requires public sector governance systems to anticipate, withstand, recover from and adapt to cyber shocks, challenging the role of assurance.

Public sector cyber-resilience reflects a broader public governance reorientation from risk prevention and control towards management of uncertainty, interdependence and disruption in complex socio-technical systems. Influential work in public management and cybersecurity studies has conceptualized resilience as a governing logic concerned not only with avoiding failure but also with sustaining essential functions under conditions of stress and transformation (Boin and Lodge, 2016; Boin and van Eeten, 2013). Cyber-resilience extends these concepts, and we draw on practitioner and policy frameworks emphasizing anticipatory preparedness, absorptive capacity, recovery and adaptive learning as interrelated capabilities (Linkov and Kott, 2019; Verma *et al*., 2025). Recent cyber incidents affecting public institutions, including ransomware attacks on the British Library, cyber breaches affecting government agencies and attacks on critical public infrastructure, demonstrate that many public organizations continue to struggle to anticipate, absorb and recover from increasingly sophisticated cyber threats (British Library, 2024; United States Government Accountability Office, 2022). Nevertheless, little is known about how performance audit (PA) can contribute to strengthening public sector cyber-resilience and support governance in responding to emergent cybersecurity risks.

Cyber-resilience poses distinctive challenges for public sector audit. Classic analyses of auditability emphasize how risks and activities are stabilized, documented and rendered amenable to verification through indicators, controls and evidence (Power, 1996). Yet cybersecurity threats are new and uniquely characterized by uncertainty, opacity and rapid mutation, with highly consequential vulnerabilities residing in infrastructures, inter-organizational interfaces and legacy systems – these threats resist neat codification (Haapamäki and Sihvonen, 2019). Moreover, cyber incidents unfold in real time and across organizational boundaries, whereas PA has traditionally operated through retrospective cycles and organization-centric scopes.

Recent studies examine SAIs' responses to digitalization and technological change, highlighting challenges related to their skills, mandates and organizational transformation (e.g. Otia and Bracci, 2022; Parker, 2023). Otia and Bracci (2022) stress that SAIs are under-equipped to address emerging cybersecurity risks, both methodologically and technically, with Rana and Parker (2023) observing that cybersecurity auditing requires hybrid skill sets, inter-organizational coordination and ongoing reconfiguration of audit mandates and expectations. While providing important insights into SAIs' institutional capacity in digital contexts, less attention is paid to how the public sector cyber-resilience imperative may reshape PA as a fundamental SAI "product". The International Organization of Supreme Audit Institutions (INTOSAI) calls for SAIs to undertake proactive engagement in auditing IT systems and supporting digital reform (INTOSAI WGITA, 2016, 2022), with the current 2026–2028 INTOSAI WGITA Work Plan focusing on cybersecurity and remote audits [1]. We shift the analytical lens to the re-specification of audit objects, practices and products under conditions of systemic digital risk, arguing that the PA function is well-positioned to evaluate not only compliance with cybersecurity protocols but also the public sector's cyber-resilience and capabilities to anticipate, absorb, recover and adapt to cybersecurity risks.

Thus, we ask: *Which performance audit practices do SAIs prioritize to address public sector cybersecurity risks and contribute to building its cyber-resilience?* To address this question, we utilize an exploratory qualitative research design combining semi-structured interviews across multiple jurisdictions, alongside documentary analysis and international training materials. This empirical strategy enables an in-depth examination of how cyber-resilience is being problematized, operationalized and enacted through evolving PA practices in high-functioning audit environments.

Cyber-resilience is a contested concept, grounded in various disciplinary perspectives; hence, Section 3 presents a working definition of public sector cyber-resilience. Through PA, we examine a selection of public sector cyber incidents indicative of those constantly peppering media reports; their impact on core infrastructure and operations and accountability "witch-hunts" (see, for example, Algemene Rekenkamer, 2020; British Library, 2024; United States Government Accountability Office, 2022). Our qualitative research includes in-depth interviews with 17 performance auditors, cybersecurity experts and public sector IT professionals. These are complemented by documentary analysis of global training materials, audit reports and international cybersecurity frameworks (including those developed by INTOSAI, the European Union (EU) and SAIs).

We find that PA is re-temporalized and re-scaled by public sector cyber-resilience. Rather than focusing primarily on retrospective assessments of controls and compliance, high-functioning SAIs increasingly orient PA towards anticipatory and system-level concerns. Empirically, this shift is expressed through the emergence of new audit objects (such as preparedness, interdependencies and recovery capacity), new audit practices (including verification of self-assessments, attacker-mindset reviews, simulations and near-real-time assurance) and new audit products (such as guidance, maturity models and cross-sector learning mechanisms). Combined, these developments reposition PA as a catalytic and infrastructural governance device in the management of cybersecurity risk.

The paper makes three contributions. *Firstly*, it extends the auditability and audit-as-catalyst literatures (Andon *et al*., 2015; Gendron *et al*., 2001; Power, 1996, 1997) by showing how PA's temporality, scale and products are reconfigured by public sector cyber-resilience imperatives demanding anticipatory, system-oriented and infrastructural advice. PA builds on its reform-oriented and performative practice to respond to adversarial, fast-evolving digital risks. *Secondly*, we contribute empirically to public sector auditing research (e.g. Andon *et al*., 2015; Gendron *et al*., 2001; Power, 1996, 1997) by documenting SAIs' experimentations with new audit objects (e.g. preparedness, interdependencies, recovery capacity), new practices (e.g. verification of self-assessments, simulations, attacker-mindset approaches) and new outputs (e.g. guidance, maturity models, restricted and dual reporting formats) in response to cybersecurity risks. *Thirdly*, it advances debates on public sector risk management and resilience (Bracci and Tallaki, 2021; Rana and Parker, 2023) by theorizing PA not merely as a mechanism of oversight but as an institutional actor that can actively shape the conditions of public sector cyber-resilience, thereby repositioning SAIs within evolving architectures of digital risk governance.

The paper continues with Section 2, reviewing the extant literature on PA and its possible adaptations to address public sector cyber-resilience and cybersecurity risks. Next, we introduce the theoretical framing of cyber-resilience used to analyse our findings. Section 4 outlines our methodological approach, followed by Section 5, which explains the presentation of the empirical findings across the four cyber-resilience goals. Section 6 theorizes the findings and articulates the study's contributions to scholarly and policy debates. Finally, in Section 7, we conclude with reflections on the implications, limitations and avenues for future research.

2. Literature review

We focus on research on PA's evolving scope in dynamic risk environments and the distinctive challenges posed by cybersecurity risk management within public institutions, thereby identifying disconnections constraining our current understanding of what SAIs should (or do) prioritize to address cybersecurity risks and support public sector cyber-resilience. Free *et al*. (2020) suggest that new PA practices are readily disseminated internationally through INTOSAI, especially amongst high-functioning SAIs. While the 3 Es of PA (economy, efficiency and effectiveness) typically focus on program outputs and accountability, prior research also posits that PA can contribute to adaptive governance and public sector resilience (Otia and Bracci, 2022; Rana and Parker, 2023). PA can intersect oversight and foresight to

assist auditees in responding to cybersecurity risks; further, prior literature highlights SAIs' abilities to enable institutional reform across the public sector (de Fine Licht, 2019), in addition to being evaluators who advise on control risk–features such as are necessary for cyber-resilience. The following literature, when combined with our theoretical framework, builds a case to answer our research question.

2.1 Performance audit, SAIs and audit's governance role

PA has long been understood as a central technology of public sector governance through which activities, programmes and organizations are rendered visible, comparable and evaluable (Power, 1996, 1997). As it matures, PA regularly reshapes problem framings, organizational attention and accountability relationships (Andon *et al*., 2015; Barbera *et al*., 2017; Gendron *et al*., 2001). From this perspective, audit is not merely a neutral instrument of verification, but a socio-technical device that participates in defining what counts as a problem, what evidence is relevant, and what kinds of interventions are legitimate.

Relatedly, PA has been conceptualized as a catalytic reform device, capable of mobilizing actors, diffusing practices and reconfiguring governance arrangements beyond the immediate audit target (Andon *et al*., 2015; Bracci and Tallaki, 2021). In this mode, PA operates beyond reporting through a broader repertoire of practices (recommendations, benchmarks, guidance and follow-up processes) to influence organizational conduct and policy priorities. Hence, PA contributes to governing "at a distance" by translating complex issues into auditable objects and actionable categories (Power, 1996), while also participating in the circulation of managerial and governance logics across the public sector (Gendron *et al*., 2001; Free *et al*., 2020).

Contemporaneously, critical scholarship emphasizes PA's limits and ambivalences. Auditability depends on entity transparency (de Fine Licht, 2019) and the stabilization and codification of activities into indicators, controls and documentary traces that can be inspected and verified (Power, 1996, 1997). Audit is not merely technical but deeply political, privileging certain forms of knowledge and action while marginalizing others. Moreover, the expansion of audit and performance measurement has been associated with ritualized forms of verification and symbolic reassurance, resulting in a decoupling between formal assurance and substantive organizational change (Gendron *et al*., 2001; Power, 1997). These studies underscore that PA is not simply an oversight tool, but a governing practice related to the nature of the problems it is called upon to address.

A recent body of work examines SAIs' and audit institutions' responses to digitalization and technological change. This literature points to challenges related to skills, data access, analytical capabilities and organizational transformation within audit offices (Otia and Bracci, 2022; Rana and Parker, 2023). While these studies provide important insights into institutional adaptation and capacity constraints, they treat digitalization primarily as a contextual challenge for existing audit practices rather than as a force that potentially reconfigures PA's very nature as a governance device.

Nevertheless, cybersecurity risk differs qualitatively from performance and compliance issues traditionally addressed by PA. As noted, cyber threats are adversarial, fast-evolving and deeply embedded in complex inter-organizational and infrastructural arrangements (Linkov and Kott, 2019; Verma *et al*., 2025). These features challenge audit models that presuppose relatively stable risk categories, bounded organizational entities and retrospective evaluation cycles. Hence, cybersecurity risk raises questions not only about audit capacity but also about the underlying logics of auditability, accountability and catalytic intervention.

Accountability for cyber-resilience lies with governments. Yet we argue that persistent cybersecurity risks, escalating digital complexity and expectations for greater public sector cyber-resilience challenge institutional roles, practices and structures within the public sector environment. Hence, crises such as large-scale cyber-attacks can be opportunities for systemic improvement (Brockner and James, 2008; Shaw and Maythorne, 2013) and transformation.

SAIs are being called upon to facilitate transformative learning, institutional redesign and collaborative governance (Bracci and Tallaki, 2021; Parker, 2023; Rana *et al.*, 2022), suggesting they could emerge as facilitators of multi-actor governance, convenors of learning spaces and translators of complex risks.

2.2 Disconnections in PA literature, cybersecurity and public sector cyber-resilience

Public administration and cybersecurity studies have increasingly invoked the concept of resilience to capture how governance should operate under conditions of uncertainty, disruption and systemic interdependence (Boin and van Eeten, 2013; Boin and Lodge, 2016). Rather than focusing solely on risk prevention or control, resilience-oriented governance emphasizes organizational capacity to anticipate shocks, absorb their impacts, recover essential functions and adapt to changing threat environments. The cybersecurity logic has been further operationalized through practitioner and policy frameworks that specify phases or goals of cyber-resilience, including preparedness, response, recovery and adaptation (Bodeau *et al.*, 2015; Linkov and Kott, 2019; NAO, 2025; NIST, 2024; Smith, 2023; Verma *et al.*, 2025).

Unlike conventional infrastructure risks, cybersecurity risks manifest as "wicked problems" that are emergent, transboundary and highly unpredictable. Representing a domain characterized by rapid technological evolution, asymmetric threats and blurred public–private boundaries, cybersecurity risks disrupt traditional audit paradigms centred on static criteria and linear causality (Otia and Bracci, 2022; Rana and Parker, 2023). Crucially, cyber-resilience foregrounds features that sit uneasily with established audit models. Firstly, rather than probabilistic or purely technical, cybersecurity risks are explicitly adversarial: threats are intelligent, adaptive and strategically oriented. Secondly, risk is systemic: vulnerabilities and failures often emerge from inter-organizational dependencies, shared infrastructures and extended digital ecosystems rather than from isolated organizational units. Thirdly, resilience is temporal: effective governance depends not only on learning from past incidents but also on anticipatory preparation and, in some cases, real-time response. Together, these features suggest that cyber-resilience is not merely another topic to include in audits. Rather, it repositions PA as a governance capability that contributes to building public sector cyber-resilience through anticipatory assurance, organizational learning and adaptive governance.

Public sector organizations face budget constraints, which, when combined with inter-agency dependencies (Shaw, 2012; Shaw and Maythorne, 2013), render them particularly vulnerable to cybersecurity risks. Yet, the public sector audit literature has scarcely addressed the practical implications of poor governance. Resilience to withstand cybersecurity risks (Linkov and Kott, 2019; Verma *et al.*, 2025) requires not only technical safeguards but also system-wide adaptive capacities, including anticipatory threat mapping, cross-agency contingency planning and digital upskilling. To contribute to the building of sectoral cyber-resilience, SAIs must reconceptualize PA to incorporate indicators of public sector organizations' cyber-resilience, such as vulnerability assessment and penetration testing, redundancy, diversity and flexibility (Comptroller and Auditor General of India, 2024; INTOSAI WGITA International Organization of Supreme Audit Institutions Working Group on IT Audit (WGITA), 2016, 2022; INTOSAI IDI Development Initiative, 2022). Nevertheless, how SAIs adapt to evaluate and build organizational cyber-resilience remains under-researched.

Despite its growing salience, the intersection of cyber-resilience, cybersecurity risks and PA remains fragmented in public governance literature (Smith, 2023). Much PA literature orients towards retrospective evaluation, even in its more catalytic and reform-focused variants (Andon *et al.*, 2015; Bracci and Tallaki, 2021; Gendron *et al.*, 2001). By contrast, cyber-resilience prioritizes anticipatory preparedness and forward-looking capacities, raising questions about how audit can intervene meaningfully before rather than only after, disruptive

events. Three key disconnections emerge: firstly, the operationalization of cyber-resilience within public sector audit practice is largely undocumented. While Duchek (2020) and Parker (2023) provide frameworks for conceptualizing resilience, scarce evidence exists of them being applied in empirical audit settings or to cyber-resilience in the public sector. Secondly, PA literature has insufficiently incorporated insights from public administration and crisis governance scholarship. Notably, intellectual siloing means the rich conceptual work on strategic resilience, paradoxical leadership and adaptive systems (Boin and van Eeten, 2013; Shaw and Maythorne, 2013) remains disconnected from empirical audit studies. Literature analyses internal MCS for building entities' resilience (e.g. Bracci and Tallaki, 2021); we analyse PA's role in encouraging cyber-resilience across the public sector. Thirdly, limited empirical work documents SAIs' adaptions of their toolboxes to address cybersecurity risks within their PA mandates. While some recent contributions (e.g. Otia and Bracci, 2022) gesture towards audit innovations, most existing studies focus on institutional challenges (e.g. skills deficits, narrow audit mandates) rather than necessary audit transformations.

A further tension concerns audit's scale and boundaries. Established audit frameworks privilege the organization as the primary unit of analysis and intervention, consistent with classic notions of auditability and accountability (Power, 1996, 1997). Cyber-resilience, however, is inherently systemic: critical vulnerabilities often reside in interfaces between organizations, in shared infrastructures and in extended supply chains. Such cross-cutting cybersecurity risk is mismatched by audit's organizational boundaries. Finally, audit scholarship examining PA's primary products has focused on its reports and formal assurance outputs (e.g. de Fine Licht, 2019; Gendron *et al*., 2001). Our empirical material exposes different "products" and tools aimed at shaping preparedness and adaptive capacity over time.

In summary, cyber-resilience challenges prior notions of auditability (Andon *et al*., 2015; Bracci and Tallaki, 2021; Gendron *et al*., 2001; Power, 1996, 1997) by its fast-moving and systemic nature and demands on governors' learning and adaptability. Combined, these features suggest that public sector cyber-resilience is an emerging PA topic, potentially re-specifying what counts as an auditable object, when audit intervenes and what audit products are considered legitimate and useful. Contributing to further developments requires cross-disciplinary dialogue and empirical inquiry, which is our intent. By examining how PA can develop public sector cyber-resilience, we confirm PAs' potential for capacity-building. Conceptualizing SAIs as cyber-resilience actors foregrounds how they can contribute to re-shaping governance, align stakeholders and catalyse organizational learning in the wake of public sector cyber crises. Furthermore, our approach supports the broader epistemological change of PA from static evaluation to dynamic facilitation of public value and anticipatory governance. Given the identified gaps and possibilities, we utilize an analytical framework of cyber-resilience to answer our research question into PA.

3. Theoretical framework

This study conceptualizes public sector cyber-resilience as a governance logic that derives from but is different from resilience. In public administration and security studies, resilience has been advanced as a way of governing under conditions of uncertainty, disruption and systemic interdependence, shifting attention from the prevention of failure towards the capacity to anticipate, absorb, recover from and adapt to shocks (Boin and Lodge, 2016; Boin and van Eeten, 2013; Parker, 2023). In addition to reactive mechanisms and static risk mitigation capabilities, resilience encompasses dynamic, anticipatory and regenerative processes that shape institutional futures through reforming, learning and recalibration in the face of volatility and uncertainty (Barbera *et al*., 2017; Rana and Parker, 2023).

Practitioner and policy frameworks operationalize cyber-resilience as a set of interrelated capabilities to achieve the goals of preparedness, response, recovery and adaptation (Linkov and Kott, 2019; NAO, 2025; NIST, 2024; Verma *et al*., 2025).

Recognizing cyber-resilience is a contested concept due to its interdisciplinarity (Linkov and Kott, 2019; Smith, 2023). Smith (2023, p. 22) defines it as "*the capabilities of cybersecurity, business continuity, and enterprise resilience*". This focuses cyber-resilience on "system coping … when prevention is impossible", with the World Economic Forum defining the key difference between cyber security and cyber-resilience as the *shift to anticipating, withstanding, and rapidly recovering from [cyber-attacks]* [2]. The UK's National Audit Office (NAO) (2025, p. 34) reflects that cyber-resilience represents "*how well an organization can continue running its most important business and services and ensure the protection of its data, despite adverse cyber security events*". Hence, as the MITRE Corporation notes, cyber-resilience extends beyond "*primarily on keeping an adversary out of a system*" (cybersecurity) to proactively establishing networks and managing operations despite some system aspects being compromised following an attack. For PA, taking a cyber-resilience logic introduces new evaluative criteria of adaptability, redundancy, interdependence and system survivability (Smith, 2023).

Pavão *et al*. (2023) review case studies in cybersecurity risk management, particularly those of organizations working towards cyber-resilience. They note that, when organizations focus on cyber-resilience as a concept, they can better "*understand the status of their organizations in terms of being able to prevent, respond and recover their normal business activity … [and thus] implement or refine resilience plans*" (Pavão *et al*., 2023, p. 315). Some of their case studies adapted the National Institute of Standards and Technology (NIST) Cybersecurity Framework (e.g. NIST, 2024) [3], while others developed new frameworks and tools to assess cyber-resilience. Another influential framework is the MITRE Cyber Resiliency Engineering Framework [4].

While our exploratory research does not aim to measure public sector cyber-resilience *per se*, we utilize the goals outlined by Linkov and Kott (2019) and Verma *et al*. (2025) to frame our investigation of PA and the aspects high-performing SAIs prioritize to address public sector cybersecurity risk management and contribute to their cyber-resilience. We analyse PA against the four analytically distinct but interrelated cyber-resilience goals: anticipation (or preparedness), absorption (or withstanding), recovery and adaptation (Linkov and Kott, 2019; Verma *et al*., 2025). These goals are not conceived as linear stages, but as overlapping and mutually reinforcing capacities that structure how public sector governors seek to be resilient against cybersecurity risks. Importantly, each goal carries distinct implications for PA's role. Beyond planning, the latter three stages (absorb/withstand, recover and adapt) differentiate cyber-resilience from cybersecurity risk management by dealing with the residual risk (Linkov and Kott, 2019; Verma *et al*., 2025). We link the various names authors use for cyber-resilience goals in Table 2 and now expand these for the public sector PA environment.

Anticipation refers to the capacity to identify, prepare for and mitigate potential cyber threats before they materialize. Resilience-oriented governance includes activities such as risk mapping, asset identification, scenario planning and developing preparedness frameworks (NAO, 2025; Smith, 2023), with such preparedness aiming to prevent and withstand potential cyber-attacks (Linkov and Kott, 2019; Verma *et al*., 2025). *Anticipation* requires PA to expand evaluation towards preparedness, foresight and organizational readiness, re-temporalizing the audit. It may legitimize new interventions required before disruptive events and position PA as a device that also scrutinizes how organizations should prepare for events they cannot fully predict. Despite the necessity of anticipation, the NAO (2025, p. 4), for example, reported to the UK government that "*systems controls fundamental to departments' cyber resilience were at low levels of maturity in 2024*", with "*significant gaps*" in planning to withstand cyber-attacks.

Absorption concerns systems' abilities to withstand and contain the impacts of cyber incidents while maintaining essential functions. This goal foregrounds issues such as incident response capabilities, continuity arrangements and the robustness of defensive architectures (Linkov and Kott, 2019; Verma *et al*., 2025). Even during an auditee's cyberattack, SAIs may be able to promote public trust, encourage ethical data use and strengthen citizens' privacy

protection rules. *Absorption* emphasizes performance under stress and disruption rather than under normal operating conditions. PA assessments of absorption can engage with simulations, stress testing and attacker-mindset assessments, thereby extending audit beyond the verification of documented procedures towards the evaluation of dynamic response capacities.

Recovery focuses on restoring functionality after a cyber incident and reconstituting compromised systems, data and services. In systemic digital environments, recovery is rarely confined to a single organization, often depending on inter-organizational coordination, supply chain relationships and shared infrastructures (Linkov and Kott, 2019; Smith, 2023; Verma *et al*., 2025). *Recovery* can be a long process in low cyber-resilient environments (NAO, 2025). With much of the public sector being organizationally interdependent, cyber-attacks spread quickly; hence, government departments, cybersecurity agencies and audit offices could work collaboratively to respond to a major cyber incident impacting multiple agencies. Yet, Lehto and Limnéll (2021, p. 143) examine the Finnish public sector, noting that the "*number of actors is large . . . strategic leadership of cybersecurity is fragmented . . . [with] no effective cooperation structure . . .*". They conclude that, despite a cybersecurity strategy, "*coherence of activities and a shared situational picture may remain incomplete*" (Lehto and Limnéll, 2021, p. 148). This common interdependence likely re-scales the PA audit object from individual organizations to the broader ecosystem within which recovery is enacted, introducing questions about accountability and responsibility allocation due to diffuse boundaries of causation and control.

Adaptation refers to the capacity to learn from cyber incidents and 'near-misses' and to reconfigure technologies, processes and governance arrangements that respond to these evolving threat environments. This goal highlights the forward-looking and transformative aspects of resilience, extending beyond incremental improvement towards fundamental changes in architectures and practices (Bodeau *et al*., 2015; Linkov and Kott, 2019; Verma *et al*., 2025). *Adaptation* blurs the PA boundary between evaluation and advice and between oversight and capacity-building. As we show, PA oriented towards adaptation may increasingly be expressed as guidance, maturity models and sector-wide learning initiatives. SAIs that experiment with agile audit practices, pilot cybersecurity maturity models and engage in real-time audits with IT experts exemplify the building of sectoral cyber-resilience – within auditees and themselves. Potential actions include cyberattack simulations, planning how to respond to new threats and encouraging governors to think strategically about digital risks. PA could emphasize horizon scanning, scenario planning and reconfiguring audit criteria to include forward-looking indicators of preparedness. Developing solutions requires learning and exploring counterfactual, counterintuitive responses. It may also signal the need for updated legislation and encourage significant infrastructural investments (NAO, 2025). Yet, adaptation activities raise questions about audit independence, mandate boundaries and appropriate audit products.

These four goals provide a framework for analysing how public sector cyber-resilience reconfigures the role of PA across time, scale and function. This framework underpins our empirical analysis and examination of how SAIs are experimenting with new audit objects, practices and products in response to the challenges of governing cybersecurity risk in contemporary public sectors. We respond to research calling for more work on how audit has transformed from episodic assessments and punitive evaluations to ongoing, dialogic engagements and co-constructed improvement pathways (Ek Österberg and Licht, 2021; Kastberg and Ek Österberg, 2017; Parker *et al*., 2021). PA that responds to cyber-resilience demands may engender necessary adaptation and learning in auditees as well as SAIs, as our empirical observations show.

4. Methodology

This study adopts an exploratory qualitative research design to examine which PA practices SAIs prioritize to address cybersecurity risks and respond to public sector cyber-resilience imperatives. Given the emergent, complex and institutionally sensitive nature of cybersecurity

governance, a multi-method qualitative research design is appropriate for capturing how actors problematize cybersecurity risk, interpret their mandates and experiment with new audit objects, practices and outputs (Parker and Northcott, 2016). Rather than seeking statistical representativeness, the study is designed to generate theoretically informed insights into evolving audit practices in high-functioning audit environments where cybersecurity risk is recognized as a strategic governance issue.

We draw on three main sources of empirical data: (1) semi-structured interviews with key stakeholders involved in public sector auditing and cybersecurity governance; (2) document analysis of national cybersecurity strategies, public audit reports and institutional guidance; and (3) content analysis of INTOSAI global training materials, particularly the 2023 "Leveraging on Technological Advancement" (LOTA) series. These sources extend our exploratory research across actors, levels and discourses to find commonalities and differences and enhance the robustness and credibility of findings. By capturing the lived experiences, rationalities and practices of diverse actors – including auditors, public IT officers and cyber regulators in various national contexts – we aim to understand how public sector cyber-resilience is constructed, enacted and challenged by SAIs' audits.

SAIs and their ecosystems were treated as embedded cases because cybersecurity risk is a socially embedded, context-specific and evolving phenomenon; it requires close examination of situated practices, logics and governance arrangements rather than large-scale survey generalization. By engaging actors at different nodes of the cybersecurity–audit nexus – auditors, CIOs and regulators – we captured both vertical (organizational and policy) and horizontal (cross-agency and inter-institutional) perspectives.

Following ethical clearance, we conducted 17 interviews between November 2023 and October 2024. Participants were purposively sampled from three categories (see Table 1):

(1) A1–A9: Public sector (SAI) auditors, predominantly in Europe/UK and Asia-Oceania. As noted in Table 1 below, five were specifically IT auditors (Directors of IT audit teams), one was an internal auditor (in a jurisdiction where internal audit is part of the SAI's mandate) and three were PA auditors.

(2) C1–C3: Chief Information Officers, of which two were from SAIs and one from an auditee. The latter was undertaken primarily to deepen our understanding of the cyber and audit context of a large public sector entity.

(3) R1–R5: Cybersecurity regulators, policymakers and standard-setters involved in shaping public sector cybersecurity frameworks. These enabled us to examine the interaction between public cybersecurity policies and PA.

Participants were purposively selected from jurisdictions with established public sector cybersecurity agendas to examine leading-edge practices rather than routine compliance. The sample spans the UK, Europe, Latin America/Caribbean and Asia–Oceania, providing variation in digital maturity, institutional independence and regulatory frameworks. Most participating SAIs were high-performing, with LOTA materials broadening coverage to some areas otherwise difficult to access.

The restricted nature of cybersecurity-related work constrained access. Cybersecurity risk is a sensitive topic, requiring us to source interviewees through professional networks, formal requests to audit institutions and referrals. Interviewees were promised anonymity, and published materials complemented this data, expanding our evidence analysis. Table 1 summarizes the interviewee profiles, pseudonyms, regional affiliations, type of audit model [5] and interview length.

Interviews were conducted using a semi-structured protocol designed to elicit participants' experiences with cyber-related audits, their perceptions of cyber-resilience, and their views on how PA practices are evolving in response to digital risk. We adapted the interview guide for each participant group while retaining a common core of themes, including preparedness and

Table 1. Interviewees, videos and pseudonyms

Alias	Area of expertise	Region	Length
Interviews			
A1	Public sector (SAI) auditor	Asia-Oceania (Westminster/ Parliamentary)	62 minutes
A2	Public sector (SAI) auditor	Europe/UK (Board/Collegial)	54 minutes
A3	Public sector (SAI) auditor	Asia-Oceania (Westminster/ Parliamentary)	32 minutes
A4	Public sector internal auditor	Europe/UK (Board/Collegial)	60 minutes
A5	Public sector (SAI) Performance Auditor	Asia-Oceania (Westminster/ Parliamentary)	30 minutes
A6	Public sector (SAI) Performance Auditor	Europe/UK (Westminster/ Parliamentary)	54 minutes
A7	Public sector (SAI) Performance Auditor	Europe/UK (Westminster/ Parliamentary)	52 minutes
A8	Public sector (SAI) Performance Auditor	Europe/UK (Board/Collegial)	62 minutes
A9	Public sector (SAI) Performance Auditor	Europe/UK (Board/Collegial)	54 minutes
C1	Chief Information Officer–SAI	Asia-Oceania (Westminster/ Parliamentary)	71 minutes
C2	Chief Information Officer–Auditee	Asia-Oceania (Westminster/ Parliamentary)	42 minutes
C3	Chief Information Officer–SAI	Latin America/Caribbean (Court/ Napoleonic)	49 minutes
R1	Cyber Regulator/Standard Setter	Asia-Oceania (Westminster/ Parliamentary)	61 minutes
R2	Cyber Regulator/Standard Setter	Asia-Oceania (Westminster/ Parliamentary)	61 minutes
R3	Cyber Regulator/Standard Setter	International (mixed)	60 minutes
R4	Cyber Regulator/Standard Setter	Europe/UK (Court/Napoleonic)	53 minutes
R5	Cyber Regulator/Standard Setter	Asia-Oceania (Westminster/ Parliamentary)	44 minutes
Videos from LOTA cybersecurity series			
V1	Performance Audit of Preparedness for Cybersecurity: Bhutan Experience. Kinley Zam Performance Auditor, SAI Bhutan	Bhutan (Westminster/ Parliamentary)	22 minutes
V2	Audit of Cybersecurity. Renato Braga, Security Information Audit Manager and Andre Torres, Cybersecurity Specialist, SAI Brazil	Brazil (Court/Napoleonic)	36 minutes
V3	Audit of Zero Trust Architecture. Jeff Knott, Assistant Director, IT and Cybersecurity and Kevin Smith Senior Analyst, IT and Cybersecurity, SAI USA	US (Westminster/Parliamentary	25 minutes
V4	Cybersecurity in a rapidly evolving Space industry. George Tountas, Senior Manager, Information Security, SES Satellites	US (Westminster/Parliamentary)	20 minutes
V5	Cybersecurity and data protection. Kareem Ismail Senior Auditor, SAI Egypt	Egypt (Court/Napoleonic)	20 minutes
V6	Cybersecurity and data protection guidelines. Roberto Hernandez Rojas Valderrama, IT Audit Director, SAI Mexico	Mexico (Westminster/ Parliamentary)	17 minutes
V7	Cybersecurity and internal auditors. José Manuel Espinoza Reyes, System Engineer, SAI Costa Rica	Costa Rica (Westminster/ Parliamentary)	25 minutes

anticipation, incident response and absorption, recovery and learning and longer-term adaptation and capability-building. This structure ensured both comparability across interviews and flexibility to pursue specific contextual issues. Open-ended questions were

designed to elicit detailed and nuanced responses. Interviews were conducted either in person or via video conferencing, depending on participants' availability and location. On average, interviews averaged 50 minutes; they were audio-recorded with consent, transcribed verbatim and appropriately anonymized to protect participants' confidentiality. Participants were provided with a copy of the transcript for further feedback or amendments.

To complement the interviews, we analysed documentary materials, including SAI reports, cybersecurity strategies, audit guidance, policy documents and INTOSAI capacity-building resources. These materials provided contextual grounding, illustrated how cyber-related audit practices are codified and diffused internationally, and complemented interview evidence in a field where operational details are often confidential. The seven LOTA cybersecurity sessions (17–36 minutes) were transcribed and analysed alongside the interviews and documentary evidence to strengthen triangulation and provide additional insight into emerging international audit practices.

We analysed over 30 documents, including national cybersecurity strategies (e.g. the UK, Australia, within the European Union and New Zealand), public audit reports from national SAIs (from the regions listed in Table 1) and relevant guidance issued by international standard-setting bodies (e.g. INTOSAI). These were in addition to those recommended by interview participants, permitting an exploration of the formal and informal discourses shaping cybersecurity, PA practices and their evolution.

Data were analysed using an iterative abductive approach combining deductive and inductive thematic coding (Braun and Clarke, 2006; Fereday and Muir-Cochrane, 2006). Deductive coding drew on the four cyber-resilience capacities and relevant public sector performance audit concepts as sensitising frameworks, while inductive analysis identified recurring themes, tensions and variations across interviews, documents and LOTA materials. Coding was iterative, allowing refinement of themes through constant comparison across data sources. To enhance methodological transparency, the Appendix provides illustrative examples of how representative interview data and documentary evidence were progressively coded and aggregated into the analytical themes presented in the Findings. Documentary and training materials were analysed alongside interview data to compare formal policy narratives with enacted audit practices.

Emerging interpretations were iteratively refined through discussion among the authors, enhancing reflexivity and analytical robustness. As well as meeting frequently to discuss the emergent findings and theoretical insights, we engaged in reflexive journaling throughout the data collection and analysis phases. We systematically documented our own assumptions, reactions and interpretive challenges, particularly in relation to normative claims concerning public sector assurance, responsibilities and cyber-resilience from different jurisdictions. Reflexive engagement was essential for acknowledging the researchers' positionality and mitigating potential biases in interpretation.

Despite the strengths of this methodological approach, we acknowledge certain limitations. The research was conducted primarily in English, potentially constraining the inclusion of perspectives embedded in non-English audit discourses. Moreover, most interviewees derived from high-performing jurisdictions in Europe and Asia-Oceania, with limited representation from SAIs in the Americas, Africa or the Middle East. Hence, the findings may not fully capture the diversity of institutional responses to cybersecurity risks globally. As we were unable to persuade some potential participants from these under-researched areas to participate in our interviews, future research would benefit from a broader comparative scope that includes underrepresented regions to enhance insights into PAs' roles in public sector cyber-resilience.

5. Findings

This section presents empirical findings regarding PA's potential roles in building public sector cyber-resilience – understood as the capacity to anticipate, withstand/absorb, recover from and adapt to cybersecurity risks. By showing how PA renders visible specific cyber-resilience vulnerabilities (including those often hidden in "back-office" infrastructures,

interdependencies and legacy architectures), the analysis highlights SAIs' work towards achieving cyber-resilience goals.

5.1 PA catalyses cybersecurity investment to anticipate cybersecurity risks

A central empirical theme is that anticipation and preparedness constitute the most developed and visible pathway through which PA contributes to the public sector's cyber-resilience. The British Library's ransomware incident offers a vivid illustration of value destruction emanating from weak anticipatory cyber-related capacities. Following hostile reconnaissance and the exfiltration of approximately 600 GB of files, the British Library faced severe disruption, destruction of servers and constrained recovery, with the attackers later auctioning the data and dumping it on the dark web. The post-incident reflection is blunt: *"... with the benefit of hindsight there is much we wish we had understood better or had prioritized differently"* (British Library, 2024, p. 18). The report also acknowledges that cyber-resilience is not reducible to technical patching; it requires "significant changes" to applications, culture and ways of working. This reflection underscores that resilience is organizational and infrastructural, as well as technological.

The British Library provides an exemplar of a broader governance pattern: weak planning is rarely accidental. It is often the outcome of long-run neglect of organizational scaffolding – legacy systems, capability deficits and cultural marginalization of cybersecurity risk as "IT's problem" [6]. PA can make such vulnerability visible by shifting the audit gaze from discrete incidents and specific failures towards the institutional and architectural conditions that either enable or undermine cyber-resilience. Such PA would extend beyond a forensic role (surfacing structural weaknesses and governance neglect) to a catalytic role (prompting reform and investment). High-functioning SAIs catalyse by evaluating and reporting on whether public entities possess the capacity to withstand high-impact cyber incidents, reorganize adaptively and ensure continuity of essential services (e.g. Comptroller and Auditor General of India, 2024; see also NAO, 2025).

This catalytic role is necessary because – despite heightened awareness – several participants reported persistent reluctance among public sector governors to allocate resources to cyber-resilience planning [7]. One auditor described the structural origins of cyber vulnerability in the public sector as a political–financial pattern rather than a technical accident:

> The bigger risks have come from some of the older systems that have been implemented, but actually a lack of investment in IT functions has meant that often the public sector has not kept up to date with security patching and access controls ... There's a perception that cybersecurity is a background IT department [role] ... there hasn't been historically an appetite to prioritize public spending on back-office functions. (Interview A2)

To reframe the urgency of infrastructural investment and expose issues for their urgency throughout the organization (not merely in the 'back-office'), PA makes cybersecurity risk auditable. It links to recognizable governance concerns – risk appetite, resource allocation, organizational accountability – rather than leaving it as an isolated technical, politically unrewarding matter. Hence, governments increasingly seek to institutionalize preparedness through mandatory organizational self-assessments against frameworks (e.g. Europe-NIS2; UK-GovAssure; Australia-Essential Eight) and by placing explicit responsibility on boards or senior executives [8]. However, our participants repeatedly problematized such self-assessment regimes as vulnerable to optimism bias, ceding to inertia. High-performing SAIs therefore use PA to verify those self-assessments independently, countering what *Interviewee A7* called the "*mark your own homework approach*". Another auditor explained:

> ... often the self-assessments provided by entities are overly optimistic. They mark themselves as compliant, but once we actually perform the audit, we uncover several areas where controls are not in place or are insufficient (Interview A2).

Furthermore, the audit contribution extends from merely management control to governance:

> . . . our role becomes crucial when it comes to verifying not just what the entities report but also testing their systems to ensure those claims are accurate. It's about assurance, not just compliance (Interview A5).

Conceptually, this demonstrates how PA re-specifies the auditable object from documented compliance with specified items to credible preparedness. Hence, it responds to more than just an agency-theory-related demand for audit towards assurance of management control for management and governors.

Anticipation is also increasingly approached through behavioural and simulation-based techniques that evaluate readiness under plausible attack conditions. Persistent phishing and social engineering illustrate why preparedness cannot be reduced to technical controls alone, but requires institutionalized awareness, training and behavioural audit. One SAI described how they routinely use simulations to identify vulnerabilities and then drive targeted training interventions, including:

> . . . courses and webinars . . . about the threats and risks of the Internet . . . We also make some phishing simulations to identify the people who are more innocent about this technique of cybersecurity. After that we stimulate these people to take online courses about cybersecurity. We try to make these simulations about three times a year.

Such practices move PA from passive inspection to testing organizational capability-in-action to build public sector resilience and prioritize readiness and anticipatory capacity.

Simulation and verification can trigger governors to authorize concrete investment in recoverability and resilience. One audit in Oceania, for example, revealed a major gap in data recovery that was not recognized internally until it was surfaced through the audit process:

> After the audit, [the auditee] realized they had no capacity to restore [any stolen] data within the window needed to resume services. That drove investment in resilience, not just compliance. (Interview A8).

This is an example where PA functions as an instrument of visibility for latent vulnerabilities. It could be augmented by new technologies such as Zero Trust Architectures (ZTA), which increase perimeter safety. ZTA remains emergent but illustrates a dual audit challenge: assessing technical integrity and spurring organizational commitment/change management. In this respect, the audit object is not merely testing an IT configuration but an institutional transformation of trust, identity and access governance.

Shifting to anticipation also entails SAIs reorienting methodologically and refocusing their own identity. Multiple accounts emphasized the development of an "offensive mindset" or "attacker's point of view" to identify architectural weaknesses that audited entities can continue to test after auditors leave. As LOTA V2 described:

> . . . planning our audit teams from attacker's point of view. We like this offensive mindset, but we do not act as a red team. [9] We also use attack as tools for reconnaissance, enumeration, vulnerability assessment, but we don't use those tools to exploit, to execute exploitation . . . So, we think like an attacker, but we don't use all the way to get things done . . . And we are always trying to use open-source tools or free tools, so that organizations could also use those when we leave.

This underscores PAs' evolving role: beyond conformity with static standards, to identify architectural gaps that compromise organizational achievement of recoverability and adaptation. Diffusible methods and toolkits become mechanisms through which PA builds capacity for anticipation. However, PA's role expansion may be bounded by SAI capability constraints (see Otia and Bracci, 2022; Rana and Parker, 2023). SAI credibility depends on whether they can mobilize the technical expertise necessary to evaluate cyber-resilience claims, as one participant emphasized:

> . . . SAIs must ensure their auditors are equipped with the right technical skills, especially in areas like IT and cybersecurity. Without this, we lose credibility when advising other entities [through PAs] on how to manage these risks. (Interview A9)

Here, international infrastructures – INTOSAI WGITA training materials, shared standards and audit protocols – function as enabling conditions to upskill uneven national capability. Efforts such as the INTOSAI's WGITA (2022) assist in addressing SAIs' shortcomings by promoting shared standards, training and audit protocols for all SAIs. For example, LOTA V6 explained the Data Projection Guidelines developed by INTOSAI WGITA for effective PA; more support is promised during 2026–2028.

Disclosure politics catalyse new PA "products". Traditionally, PA results in publications warning other organizations and diffusing learning, yet the sensitivity of cyber-related findings challenges this model. Auditor participants described sanitizing findings for public reports; the details are published confidentially, disseminated through restricted seminars and, in extreme cases, not reported at all. One interviewee described controlled sharing among trusted participants, enabling "confidential things" and good practices to circulate without public exposure:

> We also organized a seminar and invited people who were involved in our audits, and it was only accessible for those people. And then we shared some good practices so they could learn from each other . . . and then a half year later we did the same [audit] actions again to check if they had improved. So, this small group of invited people could share the more confidential things and also good practices to help them... (Interview A9).

Another described a sensitive case where reporting was restricted to an in-camera briefing to Parliament and sector guidance:

> We did an audit of a utility which I won't name, and the findings were so significant that we actually did not table a public report. We only did an in-camera briefing to Parliament . . . Unfortunately, there was no full report [to disseminate for wider learnings], but we have provided a guidance for the sector. (Interview A3).

A third explicitly noted that multiple reports are a routine practice to avoid exposing vulnerabilities publicly:

> Sometimes we also have two reports, more public reports and also more confidential reports for the organization itself to help them to recover or to implement better measures . . . you don't want to expose them, of course. (Interview A9).

These practices demonstrate that in cyber contexts, the accountability benefits of transparency (de Fine Licht, 2019) may be in tension with security imperatives – an issue we consider later in our Discussion.

Finally, the findings show increased expectations that SAIs will play a reform-oriented role by disseminating best practice and ensuring follow-up. Participants highlighted recommendation tracking, periodic reporting on implementation, and the use of Better Practice Guides to shape expectations across the sector. As one participant put it:

> SAIs need to be seen as catalysts for change. Otherwise, their reports will be just that—reports. We need follow-up mechanisms, and we need to ensure compliance. (Interview A3).

Increasingly, this catalytic role includes human factors and staff training, reflecting the widely recognized shift from perimeter vulnerabilities to socially engineered entry points. As an auditor explained:

> . . . what's happened over time is entities have gotten better and better at securing the perimeter [the planning]. So, the only way that people can get through that perimeter now is to directly go to the people . . . the biggest issue that people have is they want to be useful and they like sharing information. So, if somebody asks them things, they'll just tell them . . . A lot of cyber is beyond the

> control of the CIOs nowadays and it's more on just getting good education and enough of a control to make you more difficult to target than the next guy. (Interview A1).

A regulator similarly highlighted basic asset inventory deficits requiring ongoing improvement:

> . . . a lot of risks that have turned into issues have been as a result of people/agencies not knowing what they actually have, what their inventory is . . . (Interview R2).

These observations reinforce a key interpretation: anticipation is less about "more controls" and more about embedding cyber-resilience in individuals' and organizational routines, inventories, governance attention and investment decisions. Hence, we show that PAs' contribution to organizations' anticipation of cybersecurity risks extends beyond identifying gaps. Rather, PA increasingly makes preparedness auditable through the verification of self-assessments, simulation-based practices and the diffusion of good practice – thereby catalysing investment in redundancy, legacy modernization, training and governance attention. This re-temporalizes PA by legitimising anticipatory scrutiny. It positions SAIs as institutional actors shaping preparedness architectures in the public interest. Nevertheless, when reports remain unpublished, the transparency benefits for public accountability are diminished (although it may meet management control demands for assurance).

5.2 PA encourages absorbing/withstanding cybersecurity risks

While anticipation and preparedness dominate contemporary SAI activity, our data also evidences PA increasingly contributing to organizations' and systems' capacity to absorb/withstand cyber incidents – i.e. to continue operations, limit harm and maintain essential functions even when under attack. The Dutch Court of Audit's work on Schiphol Airport provides a powerful illustration of absorptive vulnerabilities in critical infrastructures where disruption can trigger cascading public harms. As the SAI observed:

> We were alarmed to see not only that the IT system used for [passengers'] pre-assessments is not connected to the [Ministry of Defence's cyberattack] detection capacity, but also that the timetable clearly shows that this is not going to happen in the near future. (Algemene Rekenkamer, 2020, p. 31).

The Schiphol case demonstrates that absorption requires *inter alia*, detection capacity, system integration and governance prioritization to (in the Schiphol case) protect national borders and individuals' privacy rights.

Yet, persistent and intensifying cyber threats include AI accelerating attack capabilities and lowering the cost of reconnaissance and penetration; absorption is not easy. One auditor observed that threats:

> . . . never disappear. I think they're even increasing in number. The latest one . . . [is hackers] using AI to attack organizations to create phishing emails, to just find ways to penetrate the system . . . (Interview A4).

Another emphasized how automation transforms the threat landscape, compressing the time available for detection and response:

> . . . it no longer depends on somebody going off and running a whole lot of pings . . . now they give that to a bot to do . . . When [cyber-criminals] see a new technology . . . They don't think of the positive use. They always think of the negative use . . . [In the future] we'll see the same trends–it's just going to be accelerated . . . (Interview A1).

Such fast-moving threats exacerbate strategic uncertainty, requiring greater attention to how organizations continue operations in the face of attack. Absorptive capacity requires attention to preparedness-in-action, detection linkages and operational continuity.

Yet, it seems that technology evolves faster than public sector governance and capability. PA can communicate this temporal mismatch and exploitable vulnerabilities by emphasizing governors' risk appetite and accountability. As one CIO put it:

> . . . technology has been evolving faster than governance . . . capabilities in the public sector in general . . . It's that inability to respond that is the issue. That's the problem we have to solve . . . You've still got to do that future thinking process, and I still think the public sector is a little short sighted. (Interview C1).

Another participant described how auditors deliberately translate technical deficits into accessible performance signals that can provoke governance attention:

> [and] I try to throw a spotlight on it in those sort of–in those plain English type terms by, for example, scoring [the entity] 1.7 out of five. [It] brings it into people's mind about, you know, "is that how you want to score?" (Interview A6).

PA functions as a translation device converting cybersecurity risk into auditable and contestable public management categories – risk appetite, scorecards, capability maturity and operational readiness to spur absorptive governance. Assurance pursues absorption through embedding new assurance infrastructures. Some jurisdictions are experimenting with continuous monitoring, anomaly detection and *ad hoc* audit triggers immediately following suspicious patterns appearing. A regulator described a data-analytics monitoring centre that initiates rapid audits when anomalies are detected:

> . . . the Center for Anti-Corruption Data Analytics monitors procurement data continuously. As soon as there is something suspicious . . . audit departments then initiate an *ad hoc* audit on this . . . (Interview R3).

A regulator described "*formulative type reviews*" as an alternative to waiting for breaches or annual cycles (Interview R2). Conceptually, these practices represent a re-temporalization of PA towards near-real-time assurance, aligning with the resilience logic of maintaining function under stress rather than merely planning for attack.

Moreover, emerging system-oriented approaches and agile methods empower PA. For example, Bhutan's audit of cybersecurity preparedness sought:

> . . . to ascertain the government efforts towards ensuring safe and secure, resilient cyberspace in Bhutan. And the sub-objectives were to determine the appropriateness of the cybersecurity system and whether the critical information infrastructure-the CIAs-were identified and the security measures were implemented . . . The audit approach used was a system-oriented approach . . . The methodology that was used is agile framework with scrum methodology. (LOTA V1).

The PA recommended coordinated reporting and clearer regulatory responsibility, given that prior incidents were seldom unreported, limiting national learning. Bhutan's push for accountability as to the government's absorptive capacity highlights how a system-level governance problem can benefit from adaptive audit methods.

This section has shown that PA contributes to absorbing/ withstanding cybersecurity risks by translating evolving threats into governance-relevant performance signals, by evaluating integration gaps (as in Schiphol), and – where institutional capacity permits – by moving towards embedded and agile forms of assurance. The implication is that PA can assess performance under disruption to build absorptive capacity and hold entities accountable within an environment where cyber threats remain real.

5.3 Recovery and interdependence: re-scaling the PA object

Recovery, the capacity to restore functionality and reconstitute services after cyber incidents, emerges as the public sector cyber-resilience goal that most strongly compels PA to operate beyond organizational boundaries. The US GAO's account of the SolarWinds breach and the

concurrent exploitation of Microsoft Exchange vulnerabilities demonstrates that modern cyber incidents are not isolated events; they are entangled with supply chain dependencies, platform infrastructures and geopolitically motivated threat actors. As the GAO described:

> Beginning as early as January 2019, a threat actor [the Russian Foreign Intelligence Service] breached the computing networks at SolarWinds . . . Since SolarWinds Orion was widely used in the federal government . . . this incident allowed the threat actor to breach several federal agencies' information systems . . . [Contemporaneously] Microsoft reported the exploitation or misuse of zero-day vulnerabilities [10] . . . the People's Republic of China's Ministry of State Security conducted operations utilizing these Microsoft Exchange vulnerabilities . . . allowing for persistent malicious operations even after the vulnerabilities were patched. (US GAO, 2022, pp. 14, 16).

The locus of control is de-centred, and failures propagate across ecosystems, making systemic recovery from such multi-level attacks essential. Hence, research participants repeatedly emphasized intensified dependence on third-party platforms, cloud infrastructures and data-sharing arrangements, with digital transformation eroding the conceptual boundary between organizations. As one CIO put it: ". . . *that inside, outside has gone* . . ." (Interview C1).

In this environment, recovery depends on the quality of relationships, contract governance and shared contingency arrangements. One IT professional offered a detailed account of supply chain and "fourth party" exposures, emphasising how layered dependencies create cascading vulnerability:

> . . . One of the key areas we are increasingly focusing on is the supply chain risk, because when you outsource something . . . you don't know whether it is working well or not . . . Then there's the fourth party risks . . . you can sort of stack technology on technology, on technology and if you pull out the bottom pin, the whole thing comes crashing down. (Interview C2).

This articulation is alarming but emphasizes the need to re-scale PA: to evaluate recovery capability, PA must attend to interdependencies that exceed the audited entity. Nevertheless, despite interdependence, many public sector systems remain governed "in isolation". Our data reports fragmented coordination and ambiguous responsibility-sharing, which weakens crisis recovery. One Scandinavian case captured this succinctly: "*There were response plans in each agency, but no overarching coordination. That gap was a key [PA] finding*" (Interview R3).

Such findings illustrate the push for PA to focus on the governance of inter-organizational arrangements, shared protocols, incident reporting, escalation pathways and joint exercises. Some SAIs utilize collaborative strategies to develop audit capability and enhance recovery-oriented assurance, including partnerships with universities and cross-agency networks. A regulator noted the emergence of innovation labs and focused capacity-building sites:

> In Norway they have an innovation lab . . . working with artificial intelligence, machine learning . . . Same in the US . . . to focus on something which is really difficult to solve, and where they can bring the real value. (Interview R3).

Another described an SAI partnership with a university-based cybersecurity research institute and technology lab:

> We started a partnership with the cybersecurity research institute [at a university] . . . They have a very extensive technology lab. We go, we see what's happening in the sector or in the industry and then we try to adopt that into our audit practises. (Interview A3).

Recovery-oriented PA is increasingly enabled by collaborative knowledge infrastructures, through which auditors gain situational awareness and access to advanced technical environments.

Contemporaneously, collaborative recovery-oriented work introduces challenges to SAI independence and the mandate for their work. Participants described the value of cooperation with national cybersecurity centres (NCSCs) for threat intelligence, while recognising the reputational risk of appearing too close to executive actors. One auditor stated:

> Being an independent institution means that we can't always cooperate with NCSC. But without cooperation, it is difficult to get the threat intelligence we need. (Interview A5).

A CIO framed the tension in temporal terms, distinguishing arms-length checking from the collaborative work of making things "go right":

> I think collaboration is a key element in [future PA] because that understanding is always in context and situational. There's a time for some more arms' length assessment . . . the 'I'm checking that things haven't gone wrong' but checking out how things could go right has to be collaborative. (Interview C1).

Another participant acknowledged that auditees sometimes value "consultancy-like" discussions beyond formal recommendations:

> Because [auditees] know that we see a lot of organizations' governance, they appreciate this kind of consultancy I would say. (Interview A2).

These accounts demonstrate that recovery-oriented PA often requires collaborative working, which may sit uneasily with traditional audit identities.

Overall, this section shows that the recovery goal most clearly rescales PA from organizational audit towards empowering ecosystem governance. PA contributes to this governance and agency theory demand for audit by evaluating relationship quality, responsibility allocation, shared protocols and supply chain risk governance. Yet this exposes tensions between independence and collaboration that become sharper as cyber-resilience becomes a collective rather than individual achievement. These independence challenges can mar the achievement of the audit's signalling role.

5.4 PA – can PA mobilize adaptations and learning for the public interest?

Adaptation concerns an organization's capacity to learn from incidents and near-misses, reconfigure architectures and practices and transform governance arrangements as threats evolve. Empirically, this goal is both the most consequential for long-run public sector cyber-resilience and the most contested in terms of SAIs' mandates, legitimacy and signalling ability. Several participants observed a growing misalignment between statutory mandates and the practical demands of auditing in an increasingly digitized and cyber-insecure environment.

Lacking explicit mandates for specialized cyber audits, many SAIs embed cyber themes within financial audits or general performance audits – an arrangement that weakens the urgency to recruit cyber talent or innovate methodologically. One senior auditor described this institutional lag plainly:

> We don't hire cyber-specialists, and we don't intend to hire cyber-specialists for financial audit purposes . . . but [the environment] becomes incrementally or exponentially more [complex] each year. (Interview A1).

This statement reveals a core problem-building adaptation resilience: audit logics designed for fiscal compliance must be stretched to govern fast-evolving, non-financial, technologically mediated risks. Additionally, our findings suggest that adaptation also forces a reconceptualization of the auditable entity. As Sections 5.2 and 5.3 outline, digital governance must recognize inter-organizational entanglements, cloud dependencies and shared infrastructures. Such realities challenge the confinement of PA to discrete organizations with stable control boundaries. The increased relevance of continuous monitoring, anomaly detection and near-real-time interventions shifts PA from episodic oversight towards embedded assurance supporting governance. Diverse demands for audit suggest SAIs may become nodes in broader assurance networks, helping maintain ecosystem health. Nevertheless, such potential positioning raises profound questions about independence, legitimacy, and role boundaries.

Several participants articulated a vision of SAIs becoming "foresight actors" involved in horizon scanning, threat anticipation and systemic risk awareness. Achieving this requires not

only new skills but a cultural and professional shift in audit training and identity. One interviewee argued that cyber capability should not remain an IT niche but become a general audit competence:

> That training path just needs to be embedded into the audit training path in my view . . . it's a skill and a tool of every auditor. (Interview A2).

A regulator emphasized layered causality and the need for interdisciplinarity to manage systemic risk:

> There's probably multiple factors and they're all layered upon each other. (Interview R2).

These accounts demonstrate that adaptation is as much about audit professionalization and institutional redesign as it is about adopting technical tools.

A further challenge to whether PA builds adaptive capacity concerns SAI legitimacy and the public interest. Expanding SAI activity into contentious and technically complex domains requires public and political trust, demonstrable value-add and credible communication. Yet, as shown in Section 5.1, the impact of cyber audits is often impaired by sanitized reporting, restricted circulation or in-camera briefings. Hence, a structural tension emerges: the more cyber-resilience becomes strategically significant, the more audit outputs may be constrained by security imperatives. Building adaptive capacity therefore involves developing new institutional norms to balance transparency, confidentiality and learning across the public sector.

Finally, the data indicate that SAIs' adaptive capacities are preconditions if they are to catalyse public sector adaptation in general. Only by cultivating organizational cultures open to experimentation, technological literacy and responsiveness can SAIs claim a credible role in shaping public sector accountability in the digital state. This would require, for example, revising legacy paradigms of auditability, updating methodological repertoires and negotiating new forms of legitimacy to respond to the need to evolve public sector cyber-resilience governance. Hence, adaptation is both a cyber-resilience goal, an object of audit (how public sector entities learn and transform) and a reflexive challenge for audit institutions themselves (how SAIs maintain relevance and authority under systemic digital risk).

Combined, the prior subsections evidence that the PA practices SAIs prioritize to address cybersecurity risks tend to concentrate most strongly on anticipatory preparedness and, increasingly, absorptive capacity. Recovery and adaptation require broader ecosystem governance, raising sharper tensions around independence, collaboration and controlled transparency. Our Discussion section integrates these findings to articulate their implications for audit theory and public sector risk governance, with particular attention to how cyber-resilience re-temporalizes, re-scales and re-specifies PA.

6. Discussion

The findings presented in Section 5 demonstrate that cyber-resilience is not simply an additional domain in which PA is applied; rather, it fundamentally reconfigures the underlying assumptions about what PA should evaluate, how it intervenes in public sector governance, and its potential to generate different forms of public value. While prior research has recognized that PA increasingly extends beyond traditional assessments of economy, efficiency and effectiveness towards organizational learning, institutional reform and adaptive governance (Andon *et al.*, 2015; Bracci and Tallaki, 2021; de Fine Licht, 2019; Otia and Bracci, 2022), our findings show that cyber-resilience represents a qualitatively different governance challenge. Unlike conventional audit domains, cybersecurity risks are dynamic, adversarial, highly interconnected and characterized by considerable uncertainty. Consequently, cyber-resilience requires PA to move beyond retrospective evaluations of organizational performance towards anticipatory, system-oriented and adaptive forms of assurance capable of strengthening the resilience of complex public sector ecosystems.

The empirical findings, synthesized in Table 2, are foundational for developing this broader theoretical argument. Across the four cyber-resilience capacities of preparedness, absorption, recovery and adaptation, high-functioning SAIs were found to be expanding both the scope and repertoire of PA through new audit objects (e.g. preparedness, interdependencies and recovery capability), new audit practices (e.g. verification of organizational self-assessments, simulation exercises, attacker-mindset reviews and continuous assurance techniques) and new audit products (e.g. Better Practice Guides, maturity models, restricted reporting arrangements and sector-wide learning mechanisms). Considered collectively rather than individually, these developments suggest that the urgency of cyber-resilience is reshaping the institutional logic of PA itself. Rather than functioning solely as an evaluative mechanism that judges past organizational performance, PA increasingly operates as a governance capability that contributes to building future resilience by enabling preparedness, organizational learning, institutional coordination and adaptive capacity across the public sector.

The significance of these findings extends beyond cyber auditing. They raise broader questions concerning several established debates in the accounting and public governance literature regarding auditability, the role of PA in public sector governance and the institutional arrangements through which auditing generates accountability, learning and organizational change. Existing audit scholarship has largely conceptualized auditability as rendering organizational activities visible through documentary evidence, performance indicators and verifiable controls (Power, 1996, 1997; Ek Österberg and de Fine Licht, 2021). Likewise, PA studies have progressively expanded SAIs' roles from independent evaluators towards catalysts for organizational reform and improved public governance (Andon *et al*., 2015; Bracci and Tallaki, 2021; Gendron *et al*., 2001). Parallel research on resilience has increasingly recognized that governing complex public systems requires capabilities that extend beyond prevention and control towards anticipation, adaptation and cross-organizational collaboration (Boin and Lodge, 2016; Rana and Parker, 2023). However, these three streams of literature are rarely considered collectively to explain how emerging digital risks reshape both the theory and practice of public sector auditing.

In moving beyond the empirical findings, we develop three interrelated theoretical contributions. Firstly, we argue that public sector cyber-resilience fundamentally reconfigures the nature of auditability by changing what constitutes an auditable object, how evidence is generated, and how assurance is established under conditions of systemic digital uncertainty. Secondly, we demonstrate that cyber-resilience repositions PA from a predominantly evaluative and retrospective accountability mechanism towards a catalytic governance capability that actively contributes to organizational preparedness, resilience-building and adaptive public sector governance. Thirdly, we show that cyber-resilience transforms the institutional ecology within which PA operates by increasing reliance on transnational professional networks, collaborative learning infrastructures and new accountability arrangements that balance transparency with legitimate security concerns. Taken together, these contributions suggest that cyber-resilience re-temporalizes, re-scales and re-specifies PA, thereby extending existing understandings of auditability, the catalytic role of audit and public sector governance under conditions of accelerating technological change.

6.1 Reconfiguring auditability under conditions of cyber-resilience

Our first theoretical contribution concerns the concept of auditability. Audit scholarship has long recognized that auditability is neither an inherent property of organizations nor an objective characteristic of evidence; rather, it is socially and institutionally constructed through calculative practices that render organizational activities visible, comparable and amenable to independent scrutiny (Power, 1996, 1997; Ek Österberg and de Fine Licht, 2021). Traditional conceptions of auditability assume that organizational performance can be stabilized through documentary records, measurable indicators, established procedures and observable outcomes that permit retrospective verification. Under these conditions, audit

Table 2. Linking findings to the goals and objectives of public sector cyber-resilience

Cyber-resilience goals	Evidence of SAI/PA role in building cyber-resilience
Prepare/plan/ anticipate 'Informed *preparedness'* – proactively identifying and *preventing* potential cybersecurity risks. Preparing to *withstand* the ones that are realized	*Focus on Auditees/Public Sector* - Encouraging infrastructural investment (replacing legacy vulnerabilities) - Undertaking PAs to identify systemic weaknesses and architectural gaps (4th line of defence) - Reframing cybersecurity and cyber-resilience as a pervasive and strategic governance issue - Conducting thematic PA on digital preparedness - Developing and disseminating audit recommendations, Better Practice Guides and Insight Guides to support system-wide learning - Initiating auditee training (e.g. anti-phishing campaigns) *Changes to audit methodologies/ 'products'* - Auditing self-assessments against government preparedness frameworks - Exploring continuous audit techniques (e.g. near-real-time monitoring) - Experimenting with/encouraging new technologies, including AI and ZTA (Zero Trust Architecture)
Absorb/withstand *Continuing* business operations and services in the event of a cyber-attack. Limit or *constrain* the damage of a cyber-attack on essential functions. Maintain operational integrity and security	*Focus on Auditees/Public Sector* - Continuous monitoring of suspicious activity to enable systems to be shut down if hacker cannot be stopped - Real-time assurance, network risk-mapping, integrating defensive layers, plan audits "from an attacker's view" including ethical phishing - Encouraging reporting of cyber-attacks to build sector's knowledge *Changes to audit methodologies / 'products'* - SAIs engaging in collaborative cyber PAs across jurisdictions - Aligning with INTOSAI principles on transparency, independence and future-oriented public sector governance. Case examples: Peruvian Anti-Corruption Centre, European internal audit cooperation
Recover Post-incident recovery to restore functionality efficiently and securely. *Reconstitute* compromised resources, restore operations and apply enhanced protections to prevent recurrence	*Focus on Auditees/Public Sector* - Research innovations /using universities/consultant to assist - New responsibility for SAI to foster public accountability cultures for cybersecurity *Changes to audit methodologies / 'products'* - Promote cyber-resilient relationships considering inter-connectedness of public sector and third-party risks - Build legitimacy for new conceptions of independence in an interdependent eco-system
Adapt *Transform* technology, processes and controls, from tactical modifications to *re-architecting* systems to build public sector resilience. Proactivity is required to evolve to meet new challenges and effectively mitigate risks	*Focus on Auditees/Public Sector* - Inter-organizational relationships may compound cybersecurity risk due to shared systems and dependencies. SAI works on cross-agency cooperation, which is critical to build collective cyber resilience *Changes to audit methodologies / 'products'* - Undertake consultancy to advise on cyber governance – though this may challenge traditional norms of auditor independence - Reconfigure mandates to enable sector cyber-resilience (including increased legitimacy for such consultancy and collaborative roles)

derives its authority from the capacity to examine evidence after decisions have been made and to evaluate whether organizational actions conform to prescribed standards of performance, accountability and control.

Our findings suggest that these assumptions become increasingly problematic when applying PA to public sector cyber-resilience. Unlike many traditional audit domains, cybersecurity risks are dynamic, adversarial and characterized by continual technological change. Threat actors intentionally conceal vulnerabilities, exploit unknown weaknesses and adapt their methods more rapidly than conventional audit cycles can accommodate. Consequently, the most significant risks frequently reside not in documented controls but in latent organizational capabilities, technological interdependencies, legacy infrastructures and behavioural practices that remain largely invisible to conventional audit techniques. Cyber-resilience therefore challenges one of the central assumptions underpinning auditability: that the objects of audit can be rendered sufficiently stable for independent verification through documentary evidence alone.

Rather than demonstrating PAs' limitations, however, our findings show that SAIs reconstruct the conditions under which cyber-resilience becomes auditable. In this respect, cyber-resilience does not simply expand the range of audit topics; it transforms the epistemological basis upon which audit evidence is generated and validated. High-functioning SAIs increasingly redefine auditable objects away from the existence of cybersecurity policies or formal compliance arrangements, towards assessing the credibility of organizational preparedness, the robustness of governance capabilities and the capacity of public organizations to anticipate, withstand and recover from future cyber disruptions. As illustrated throughout Section 5, preparedness itself becomes an object of audit rather than merely a managerial aspiration. Audit attention consequently shifts from asking whether prescribed controls exist, towards whether those controls are likely to function effectively under conditions of stress, uncertainty and technological disruption.

This shift fundamentally changes audit evidence. Existing studies have emphasized that auditability depends upon making organizational activities visible through documentation and calculative representations (Power, 1996, 1997). Our findings indicate that cyber-resilience increasingly requires performative forms of verification, garnering evidence from organizational action rather than documentary representation. Practices such as phishing simulations, attacker-mindset reviews, penetration exercises, verification of organizational self-assessments, maturity assessments and scenario testing do not merely confirm existing evidence; they actively produce new evidence regarding cyber-resilience under realistic operational conditions. Auditability, therefore, becomes progressively performative rather than exclusively documentary. Audit's authority derives not only from examining historical records but also from testing whether organizations can perform effectively when confronted with evolving cyber threats. We extend existing understandings of auditability by demonstrating that audit increasingly constructs visibility through experimentation, simulation and behavioural verification.

Importantly, the empirical findings also suggest that preparedness should be understood as a dynamic governance capability rather than a static organizational condition. Existing audit practices have often privileged compliance with predefined standards, yet cyber-resilience requires continual learning, capability development and organizational adaptation. Consequently, preparedness cannot be satisfactorily evaluated through periodic inspection alone. Instead, it must be assessed through repeated processes of verification, organizational learning and capability refinement. Our findings therefore suggest that PA contributes to cyber-resilience not simply by identifying deficiencies but by making preparedness visible as an ongoing object of governance. In doing so, PA broadens its traditional evaluative role and becomes increasingly concerned with shaping future organizational capability rather than solely assessing past organizational performance.

A further implication emerging from our findings concerns organizational visibility itself. Audit scholarship has traditionally associated transparency with accountability, assuming that broader public disclosure enhances democratic oversight and institutional legitimacy

(de Fine Licht, 2019). Cyber-resilience complicates this relationship. Throughout our interviews, participants repeatedly described situations in which unrestricted disclosure of audit findings could inadvertently expose vulnerabilities, weaken critical infrastructure or provide valuable intelligence to malicious actors. Consequently, several SAIs reported developing differentiated reporting arrangements, including confidential technical reports, restricted seminars, in-camera parliamentary briefings and sector-wide guidance documents that disseminate lessons without disclosing operational vulnerabilities.

These practices indicate that cyber-resilience introduces a fundamental tension between transparency and security that existing audit theory has only partially recognized. Rather than maximising visibility, PA increasingly requires what might be described as calibrated visibility – the selective disclosure of information according to its contribution to both public accountability and collective security. Under such conditions, accountability is not diminished but reconstituted. Public reporting remains important, yet it is supplemented by alternative accountability mechanisms that facilitate organizational learning while protecting sensitive information. Better Practice Guides, aggregated sector findings, confidential recommendations and targeted capability-building initiatives emerge as complementary accountability products through which audit simultaneously fulfils its public-interest mandate and mitigates the risks associated with unrestricted disclosure. This insight extends Power's (1996, 1997) foundational proposition that auditing itself constructs organizational visibility. Our findings suggest that, in cyber-resilience contexts, the challenge is no longer purely rendering organizations visible but also determining what **should** be made visible, **to whom** and **under what conditions**. Auditability therefore becomes contingent upon balancing competing governance objectives of openness, learning, institutional trust and national security. The resulting audit process is characterized less by universal transparency than by carefully calibrated disclosure designed to maximize public value while minimising systemic vulnerability.

6.2 Repositioning PA as a governance capability

Our second theoretical contribution extends the literature that conceptualizes PA as a catalyst for organizational learning, institutional reform and improved public governance (Andon *et al*., 2015; Barbera *et al*., 2017; Bracci and Tallaki, 2021; Gendron *et al*., 2001). While prior studies demonstrate that PA shapes organizational behaviour by influencing managerial attention, legitimising reform agendas and facilitating accountability, our findings suggest that cyber-resilience expands this catalytic role. Rather than functioning primarily as an external accountability mechanism, PA increasingly operates to lift governance capability and contribute directly to building public sector cyber-resilience.

This expanded role reflects the distinctive nature of cyber-resilience, where preparedness depends not on periodic compliance reviews but on continuous organizational learning, capability development, technological adaptation and cross-organizational coordination. Consequently, PA contributes not merely by evaluating resilience but by strengthening the governance arrangements through which resilience is developed and sustained. We show that SAIs encourage investment in digital infrastructure, expose systemic weaknesses in legacy systems, elevate cybersecurity risk to a strategic governance issue and foster organizational learning through Better Practice Guides, maturity models, workshops and follow-up reviews. In doing so, PA shapes organizational priorities, governance cultures and resource allocation rather than simply reporting deficiencies.

Indeed, this catalytic role is exercised by translating highly technical cybersecurity risks into governance-relevant concepts such as preparedness, capability maturity, service continuity and leadership responsibility. Independent verification of organizational self-assessments enhances the credibility of resilience-related decision-making, while repeated engagements, recommendation tracking and sector-wide dissemination of lessons sustain organizational improvement and diffuse practical knowledge across the public sector. These mechanisms demonstrate that PA increasingly governs through capability-building rather than

compliance verification alone. In doing so, our study extends work by Bracci and Tallaki (2021), showing how PA catalyses the development of resilience-oriented management control systems through continuous monitoring, adaptive governance practices, workforce capability development and organizational learning.

We also reveal an important institutional tension. As PA becomes more involved in shaping organizational capabilities and governance architectures, the boundary between independent assurance and advisory activity becomes less distinct. Rather than representing a weakness, this tension reflects the realities of resilience governance, where cybersecurity risks are distributed across interconnected technological and organizational systems that require collaboration among SAIs, cybersecurity agencies, regulators and audited entities. Auditor independence therefore requires reconceptualization rather than abandonment. PAs' legitimacy depends less on maintaining institutional distance than on preserving professional independence while contributing constructively to collective resilience. Hence, our findings reposition PA within the broader architecture of public governance. Existing audit-as-catalyst scholarship has emphasized auditing's capacity to stimulate organizational reform and accountability. We extend this literature by demonstrating that, under conditions of systemic cybersecurity risk, PA functions to lift governance capability, assisting in constructing the institutional conditions through which resilience becomes possible. PA not only evaluates governance but also contributes to governing by strengthening organizational preparedness, fostering resilience-oriented management control systems and enabling adaptive public sector governance. As governments increasingly adopt regulatory approaches centred on continuous assurance, third-party risk oversight and whole-of-government cyber governance, these findings highlight the importance of investing not only in organizational cyber capability but also in SAIs' professional expertise, methodological capacity and institutional development.

6.3 Transforming the institutional ecology of PA

Our third theoretical contribution concerns the institutional ecology within which PA evolves in response to the urgent need for cyber-resilience. Audit practices do not develop in organizational isolation but within broader professional and transnational fields shaped by shared norms, regulatory infrastructures and institutional learning (Free *et al*., 2020; Gendron *et al*., 2001). While prior research recognizes that these fields facilitate methodological convergence, we show that cyber-resilience intensifies their importance by increasing dependence on collaborative learning infrastructures, transnational capability development and institutional coordination. Because cyber threats transcend organizational and national boundaries, the capacity of individual SAIs to conduct effective cyber-related audits increasingly requires their participation in international professional communities rather than depending on internally generated expertise alone. PA, therefore, evolves from a predominantly national accountability practice into an increasingly transnational governance activity.

This transformation is particularly evident in the role of international professional infrastructures, especially INTOSAI and its WGITA. Our findings extend previous research by demonstrating that these networks do more than disseminate good practice; they actively build audit capability through guidance, LOTA programmes, shared methodologies and collaborative cyber audits. Contemporaneously, transnational diffusion extends beyond formal standards to include methodological repertoires such as attacker-mindset auditing, simulation-based assurance, maturity assessments and continuous monitoring. Innovation in cyber auditing is therefore less a product of isolated organizational experimentation than of collective institutional learning across interconnected audit communities. However, diffusion is neither automatic nor uniform. Capability asymmetries, including shortages of cyber specialists, technological resources and financial capacity, shape the extent to which innovative audit practices can be adopted. International professional networks partially mitigate these disparities through shared knowledge, training and collaborative audit

arrangements, yet adoption remains conditioned by legislative mandates, organizational maturity and national cyber governance contexts. Consequently, PAs' institutional ecology is characterized by both convergence and diversity. Audit innovations diffuse across jurisdictions, but they are translated and adapted to local constitutional, political and organizational conditions rather than uniformly replicated.

Cyber-resilience also reshapes the foundations of institutional legitimacy. While audit legitimacy has traditionally rested on constitutional independence, procedural rigor and public transparency, our findings indicate that effective cyber-related auditing increasingly depends on technical competence, collaborative credibility and trusted relationships with specialist cybersecurity agencies. With legitimacy evolving to foreground relational practise, professional expertise and institutional independence, it raises audit mandate questions. Activities such as facilitating organizational learning, disseminating sector-wide guidance and supporting preparedness may extend beyond conventional interpretations of PA. Rather than representing inappropriate mandate expansion, however, these developments reflect institutional adaptation to interconnected and transboundary governance challenges. As the governance object shifts from individual organizations to complex digital ecosystems, audit institutions must support collective learning while concurrently maintaining independent assurance. Thus, our findings extend field-dynamics scholarship by demonstrating that cyber-resilience transforms not only audit practice but also the institutional ecology through which PA develops, acquires legitimacy and builds capability. Audit capability increasingly emerges through transnational professional infrastructures, innovation diffuses through collaborative institutional learning and legitimacy depends on the combination of independence, technical competence and adaptive governance. Understanding PAs' future evolution therefore requires moving beyond organization-centred perspectives towards an institutional ecology in which knowledge, capability and legitimacy continuously co-evolve across interconnected public sector systems.

7. Conclusion

This study examined how SAIs prioritize PA practices to address cybersecurity risks and strengthen public sector cyber-resilience. We demonstrate that cyber-resilience is not simply another audit topic; it fundamentally reconfigures PA in three interrelated ways. It re-temporalizes PA by shifting the audit focus from retrospective evaluation towards anticipatory preparedness and, increasingly, continuous assurance; re-scales PA by expanding audit attention from organization-specific controls to interconnected digital infrastructures and governance ecosystems; and re-specifies audit products by complementing formal reports with guidance, maturity models, simulation exercises and sector-wide learning mechanisms. Collectively, these shifts reposition PA from a predominantly retrospective accountability mechanism towards a governance capability that actively contributes to building public sector cyber-resilience.

The study makes three principal contributions. Firstly, it extends auditability scholarship by demonstrating that auditability must be reconsidered when the object of governance is dynamic, adversarial and systemically interconnected cybersecurity risk. Secondly, it advances audit-as-catalyst scholarship by showing that PA functions not only as a mechanism of accountability but also as a governance capability that strengthens organizational preparedness, promotes resilience-oriented management control systems and facilitates adaptive public sector governance. Thirdly, the study extends field-dynamics perspectives by demonstrating that cyber-resilience transforms the institutional ecology of PA. Audit capability increasingly develops through transnational professional infrastructures, collaborative learning networks and evolving institutional mandates that collectively shape how cyber-related audit knowledge, legitimacy and practice diffuse across jurisdictions. Beyond these theoretical contributions, the study provides rare multi-actor evidence of how SAIs operationalize cyber-resilience through verification of organizational self-assessments, simulation-based assurance, ecosystem-oriented auditing and new audit products that promote organizational learning beyond conventional audit reporting.

Certain limitations should be acknowledged. Firstly, cybersecurity auditing necessarily involves restricted access to highly sensitive information. Consequently, some highly significant audit findings cannot be publicly disclosed without increasing organizational or national vulnerability, hence restricting what we used as empirical data. As demonstrated throughout this study, SAIs disseminate cyber-related audit findings through sanitized public reports, confidential technical reports, restricted seminars and in-camera parliamentary briefings rather than full public disclosure. This reflects a structural tension between transparency-based accountability and the security requirements of adversarial digital environments (de Fine Licht, 2019). Secondly, the study primarily examines relatively high-performing SAIs operating within jurisdictions characterized by comparatively mature audit institutions and established cyber governance arrangements. Accordingly, the findings should be interpreted as analytically transferable rather than statistically generalizable. Although institutional capacities, legislative mandates and professional resources differ jurisdictionally, the mechanisms we identified, including the reconfiguration of auditability, the governance capability of PA and the importance of transnational professional learning, are likely to be relevant across a wide range of public sector settings. Indeed, they may be particularly valuable in jurisdictions experiencing higher exposure to cyber threats or greater dependence on critical digital infrastructure, where anticipatory assurance, inter-organizational coordination and resilience-oriented governance become even more important. Nevertheless, the operationalization of these mechanisms will inevitably vary according to institutional arrangements, resource availability, SAI mandates and levels of digital maturity. Future comparative research would further refine and extend these findings. Thirdly, although cyber-resilience provided the conceptual lens for this study, the research did not seek to test competing resilience theories or establish causal relationships. Instead, it offers an interpretive account of how PA contributes to resilience-building within contemporary public sector governance.

These limitations suggest several directions for future research. Comparative studies across jurisdictions with differing cyber-risk profiles and institutional capacities would improve understanding of how legislative mandates, resources and professional infrastructures influence the adoption of resilience-oriented audit practices. Further research should also examine the politics underpinning cyber-related audit disclosures, particularly how SAIs balance transparency, confidentiality and public accountability under conditions of heightened cybersecurity risk. Additionally, greater attention should be given to the governance of third- and fourth-party digital dependencies and to how auditors can evaluate ecosystem resilience without compromising their independence. Finally, processual and ethnographic studies of cyber-related audits would provide valuable insights into how auditability is practically constructed through negotiation, simulation and organizational learning under conditions of uncertainty. As governments become increasingly dependent upon complex digital infrastructures, cyber-resilience will become a defining challenge for public sector governance. This study suggests that the future contribution of PA lies not only in evaluating organizational performance but also in strengthening the institutional capacities through which governments anticipate, absorb, recover from and adapt to cyber disruption. Building cyber-resilient states therefore requires more than technological investment or stronger internal controls. It requires audit institutions to be capable of fostering organizational learning, supporting adaptive governance and sustaining public accountability within increasingly interconnected digital ecosystems.

Appendix

Illustrative coding process from raw data to analytical themes

This appendix provides illustrative examples of how interview data and documentary evidence were progressively coded and aggregated into the analytical themes reported in the paper. The coding process combined inductive identification of recurring concepts with deductive interpretation informed by the cyber-resilience framework (planning, absorbing, recovering and adapting). The examples below are illustrative rather than exhaustive.

Table A1. Illustrative examples of how representative interview data and documentary evidence were progressively coded and aggregated into the analytical themes presented in the Findings

Raw data (interview excerpt)	Initial coding	Focused code/ analytical category	Cyber-resilience capacity	Final analytical theme
Most agencies complete cyber self-assessments, but we always verify them independently because organizations often overestimate their preparedness	Independent verification; self-assessment validation; preparedness assessment	Independent assurance of organizational preparedness	Planning / Preparedness	Reconfiguring auditability through capability-oriented evaluation
We increasingly use tabletop exercises and simulated attacks to see whether organizations can actually respond rather than simply relying on written policies	Simulation exercises; testing capability; preparedness verification	Performative testing of cyber capability	Planning / Absorption	Reconfiguring auditability through performative testing
Legacy IT systems remain one of the biggest risks we encounter. Many agencies simply don't have the resources to modernize them	Legacy infrastructure; systemic vulnerability; investment need	Identifying systemic governance weaknesses	Planning / Adaptation	PA as a governance capability for resilience-building
Our Better Practice Guides often have a greater impact than the audit report because agencies use them to redesign their own cyber governance	Better Practice Guides; organizational learning; guidance	Diffusion of organizational learning	Adaptation	PA as a governance capability
Cyber incidents don't stop at organizational boundaries. We have to examine vendors, shared platforms and inter-agency dependencies	Ecosystem risk; interdependency; supply-chain governance	Ecosystem-oriented auditing	Recovery / Adaptation	Expanding audit objects beyond organizational boundaries
Much of what we learn cannot appear in public reports. We discuss sensitive findings through restricted briefings or closed seminars	Restricted reporting; confidentiality; sensitive information	Balancing transparency and security	Recovery	Calibrated visibility and public accountability
WGITA and LOTA have been invaluable because no single SAI can develop cyber expertise alone	International collaboration; shared learning; professional networks	Transnational capability development	Adaptation	Transforming the institutional ecology of performance audit
Some smaller audit offices struggle because they simply cannot recruit cyber specialists	Resource constraints; capability asymmetry	Uneven institutional capability	Adaptation	Capability asymmetries in cyber-related performance auditing

Notes

1. "INTOSAI's 2026–28 Work Plan: Pioneering Cybersecurity and IoT Audits" downloaded from: https://www.devdiscourse.com/article/technology/3796946-quantum-leap-amaravatis-vision-as-a-global-quantum-hub.
2. "Understanding Cyber Resilience with the World Economic Forum" downloaded from: https://www.splunk.com/en_us/blog/security/understanding-cyber-resilience-with-the-wef.html
3. In the International Journal of Government Auditing, Teodoro Consulting argues SAIs should use NIST principles for cybersecurity audits (see https://intosaijournal.org/journal-entry/strengthening-public-sector-cybersecurity-audits-leveraging-nist-standards-for-supreme-audit-institutions/).
4. The current version is at: https://www.mitre.org/sites/default/files/2021-11/prs-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf. The MITRE Corporation has also developed a cyber-security navigator to guide systems design – see https://crefnavigator.mitre.org/navigator.
5. While Cordery and Hay (2020) acknowledge the diversity within structure and nomenclature, SAIs are typically grouped into Board/Collegial (collective decision-making with strong audit and sanction powers), Court/Napoleonic (Court of Accounts which makes judicial rulings) and Westminster/Parliamentary (Auditor General reports to parliament but has no judicial powers).
6. See also NAO (2025), which outlines that, as at March 2024, UK government departments operated at least 228 legacy systems, yet more than 50% of the cyber security roles in departments were vacant.
7. Such under-investments are also highlighted in numerous post-cyber-attack reports, e.g. the NAO reports that three years before the May 2017 "Wannacry" ransomware infected numerous UK National Health Service (NHS) Trusts, despite warnings to upgrade NHS software by both the Cabinet Office and the Department of Health and Social Care; further NHS Digital issued warnings in the weeks prior to the attacks (see: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/).
8. The UK Government's Cyber Security and Resilience Bill to Parliament passed its first reading on 12 November 2025. It aims to increase requirements on UK public sector organizations, including aligning with the EU's regulations on NIST2 (see https://www.gov.uk/government/collections/cyber-security-and-resilience-bill).
9. Red teams comprise security professionals who simulate real-world attacks to test an organization's defences against an unseen attacker.
10. Zero-day vulnerabilities are software or hardware flaws that are unknown to the vendor and for which no patch or remediation is immediately available. Malicious actors exploit these security flaws to disrupt operations, install malware or exfiltrate data. The term means the vendor has zero days to fix the flaw before actors can exploit it.

References

Algemene Rekenkamer (2020), "Cyber security of border controls operated by Dutch border guards at amsterdam Schiphol Airport",

Andon, P., Free, C. and O'Dwyer, B. (2015), "Annexing new audit spaces: challenges and adaptations", *Accounting, Auditing and Accountability Journal*, Vol. 28 No. 8, pp. 1400-1430, doi: 10.1108/AAAJ-01-2015-1932.

Barbera, C., Jones, M., Korac, S., Saliterer, I. and Steccolini, I. (2017), "Governmental financial resilience under austerity in Austria, England and Italy: how do local governments cope with financial shocks?", *Public Administration*, Vol. 95 No. 3, pp. 670-697, doi: 10.1111/padm.12350.

Bodeau, D., Graubart, R., Heinbockel, W. and Laderman, E. (2015), "Cyber resiliency engineering aid - the updated cyber resilience engineering framework and guidance on applying cyber resiliency techniques", available at: https://www.mitre.org/sites/default/files/2021-11/prs-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

Boin, A. and Lodge, M. (2016), "Designing resilient institutions for transboundary crisis management: a time for public administration", *Public Administration*, Vol. 94 No. 2, pp. 289-298, doi: 10.1111/padm.12264.

Boin, A. and van Eeten, M.J.G. (2013), "The resilient organization", *Public Management Review*, Vol. 15 No. 3, pp. 429-445, doi: 10.1080/14719037.2013.769856.

Bracci, E. and Tallaki, M. (2021), "Resilience capacities and management control systems in public sector organizations", *Journal of Accounting and Organizational Change*, Vol. 17 No. 3, pp. 332-351, doi: 10.1108/JAOC-10-2019-0111.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: 10.1191/1478088706qp063oa.

British Library (2024), "Learning lessoons from the Cyber-attack: British library cyber incident review",

Brockner, J. and James, E.H. (2008), "Toward an understanding of when executives see crisis as opportunity", *Journal of Applied Behavioral Science*, Vol. 44 No. 1, pp. 94-115, doi: 10.1177/0021886307313824.

Comptroller and Auditor General of India (2024), "Manual on information systems (IS) Audit 2024: a Practitioner's guide", available at: https://www.cag.gov.in/uploads/media/Soft-copy-of-the-Information-Systems-Audit-Manual-2024-0684fc903e71b25-85261962.pdf

Cordery, C.J. and Hay, D.C. (2020), *Public Sector Audit*, Routledge.

de Fine Licht, J. (2019), "The role of transparency in auditing", *Financial Accountability and Management*, Vol. 35 No. 3, pp. 233-245, doi: 10.1111/faam.12193.

Duchek, S. (2020), "Organizational resilience: a capability-based conceptualization", *Business Research*, Vol. 13 No. 1, pp. 215-246, doi: 10.1007/s40685-019-0085-7.

Ek Österberg, E. and Licht, J.D.F. (2021), "Beyond auditor and auditee: exploring the governance of performance in eldercare", *Public Management Review*, pp. 1-20, doi: 10.1080/14719037.2021.1937686.

Fereday, J. and Muir-Cochrane, E. (2006), "Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development", *International Journal of Qualitative Methods*, Vol. 5 No. 1, pp. 80-92.

Free, C., Radcliffe, V.S., Spence, C. and Stein, M.J. (2020), "Auditing and the development of the modern state", *Contemporary Accounting Research*, Vol. 37 No. 1, pp. 485-513, doi: 10.1111/1911-3846.12497.

Gendron, Y., Cooper, D.J. and Townley, B. (2001), "In the name of accountability - state auditing, independence and new public management", *Accounting, Auditing and Accountability Journal*, Vol. 14 No. 3, pp. 278-310, doi: 10.1108/eum0000000005518.

Gordon, L.A., Loeb, M.P., Sohail, T., Tseng, C.Y. and Zhou, L. (2008), "Cybersecurity, capital allocations and management control systems", *European Accounting Review*, Vol. 17 No. 2, pp. 215-241, doi: 10.1080/09638180701819972.

Haapamäki, E. and Sihvonen, J. (2019), "Cybersecurity in accounting research", *Managerial Auditing Journal*, Vol. 34 No. 7, pp. 808-834, doi: 10.1108/MAJ-09-2018-2004.

International Organization of Supreme Audit Institutions Working Group on IT Audit (WGITA) (2016), "Get.it: governance evaluation techniques for information technology: a WGITA guide for supreme audit institutions", available at: http://www.tcu.gov.br

International Organization of Supreme Audit Institutions Working Group on IT Audit (WGITA) (2022), "Cybersecurity and data protection guideline",

INTOSAI IDI Development Initiative (2022), "International organization of supreme audit institutions working group on IT audit (WGITA)", *Handbook on IT Audit for Supreme Audit Institutions (2022 Revision)*.

Kastberg, G. and Ek Österberg, E. (2017), "Transforming social sector auditing – they audited more, but scrutinized less", *Financial Accountability and Management*, Vol. 33 No. 3, pp. 284-298, doi: 10.1111/faam.12122.

Lehto, M. and Limnéll, J. (2021), "Strategic leadership in cyber security, case Finland", *Information Security Journal*, Vol. 30 No. 3, pp. 139-148, doi: 10.1080/19393555.2020.1813851.

Linkov, I. and Kott, A. (2019), "Fundamental concepts of cyber resilience: introduction and overview", in Kott, A. and Linkov, I. (Eds), *Cyber Resilience of Systems and Networks*, Springer International Publishing, p. 1, available at: http://www.springer.com/series/13439

National Audit Office (2025), *Government Cyber Resilience Cabinet Office Report*.

National Institute of Standards and Technology (2024), "The NIST Cybersecurity framework (CSF) 2.0", doi: 10.6028/NIST.CSWP.29.

Otia, J.E. and Bracci, E. (2022), "Digital transformation and the public sector auditing: the SAI's perspective", *Financial Accountability and Management*, Vol. 38 No. 2, pp. 252-280, doi: 10.1111/faam.12317.

Parker, L.D. (2023), "Third sector crisis management and resilience: reflections and directions", *Financial Accountability and Management*, Vol. 40 No. 3, pp. 326-343, doi: 10.1111/faam.12379.

Parker, L.D. and Northcott, D. (2016), "Qualitative generalising in accounting research: concepts and strategies", *Accounting, Auditing and Accountability Journal*, Vol. 29 No. 6, pp. 1100-1131, doi: 10.1108/AAAJ-04-2015-2026.

Parker, L.D., Schmitz, J. and Jacobs, K. (2021), "Auditor and auditee engagement with public sector performance audit: an institutional logics perspective", *Financial Accountability and Management*, Vol. 37 No. 2, pp. 142-162, doi: 10.1111/faam.12243.

Pavão, J., Bastardo, R., Carreira, D. and Pacheco Rocha, N. (2023), "Cyber resilience, a survey of case studies", *Procedia Computer Science*, Vol. 219 No. 219, pp. 312-318, doi: 10.1016/j.procs.2023.01.295.

Power, M.K. (1996), "The audit explosion", in *Demos*, White Dove Press, doi: 10.1111/j.1467-9930.2003.00147.x.

Power, M.K. (1997), *The Audit Society: Rituals of Verification*, Oxford University Press.

Rana, T. and Parker, L.D. (2023), "Management control systems and risk management: mapping public sector accounting and management research directions", in Rana, T. and Parker, L.D. (Eds), *The Routledge Handbook of Public Sector Accounting*, Routledge, pp. 279-295.

Rana, T., Steccolini, I., Bracci, E. and Mihret, D.G. (2022), "Performance auditing in the public sector: a systematic literature review and future research avenues", *Financial Accountability and Management*, Vol. 38 No. 3, pp. 337-359, doi: 10.1111/faam.12312.

Shaw, K. (2012), "The rise of the resilient local authority?", *Local Government Studies*, Vol. 38 No. 3, pp. 281-300.

Shaw, K. and Maythorne, L. (2013), "Managing for local resilience: towards a strategic approach", *Public Policy and Administration*, Vol. 28 No. 1, pp. 43-65, doi: 10.1177/0952076711432578.

Smith, S.C. (2023), *Toward a Scientific Definition of Cyber Resilience*.

Sundberg, L. and Holmström, J. (2024), "Fusing domain knowledge with machine learning: a public sector perspective", *Journal of Strategic Information Systems*, Vol. 33 No. 3, 101848, doi: 10.1016/j.jsis.2024.101848.

Twizeyimana, J.D. and Andersson, A. (2019), "The public value of E-Government – a literature review", *Government Information Quarterly*, Vol. 36 No. 2, pp. 167-178, doi: 10.1016/J.GIQ.2019.01.001.

United States Government Accountability Office (2022), *Cybersecurity Federal Response to SolarWinds and Microsoft Exchange Incidents*, Report to Congressional Addressees United States Government Accountability Office.

Verma, P., Newe, T., O'Mahony, G.D., Brennan, D. and O'Shea, D. (2025), "Toward a unified understanding of cyber resilience: concepts, strategies, and future directions", *IEEE Access*, Vol. 13, pp. 49945-49965, doi: 10.1109/ACCESS.2025.3551887.

Wirtz, B.W. and Weyerer, J.C. (2017), "Cyberterrorism and cyber attacks in the public sector: how public administration copes with digital threats", *International Journal of Public Administration*, Vol. 40 No. 13, pp. 1085-1100, doi: 10.1080/01900692.2016.1242614.

Accounting, Auditing & Accountability Journal

Corresponding author
Carolyn J. Cordery can be contacted at: carolyn.cordery@vuw.ac.nz