Available on: http://gjetr.ep-journals.org/ E-ISSN: 3051-3782, P-ISSN: 3051-3774

Global Journal of Engineering and Technology Review

Volume: 02 Issue: 09 September 2026

The Compliance Gap: Why Audit-Based Cybersecurity Models Fail Critical Infrastructure and the Case for Continuous Control

Chukwunenye Amadi
Independent Researcher, USA

Published Date: September 10, 2026 **Article DOI : 10.65150/EP-gjetr/V2E9/2026-12**

ABSTRACT: Critical infrastructure (CI) sectors, including energy, water, transportation, healthcare, telecommunications, and finance, continue to anchor their cybersecurity assurance in periodic, audit-based compliance: scheduled assessments that certify, at a point in time, that mandated controls exist and are documented. This conceptual review argues that this model is structurally incapable of guaranteeing security in modern CI environments and develops the case for a transition to continuous monitoring and continuous control. Drawing on standards literature, empirical studies of operational technology (OT) security, documented attacks on industrial systems, and the continuous auditing tradition in accounting information systems, the paper synthesizes five interlocking failure modes of periodic compliance: (a) the static-snapshot problem, in which audit findings describe a past state rather than the present one; (b) the error-proneness and limited depth of manual, checklist-driven assessment; (c) configuration drift, through which compliant systems silently degrade between audits; (d) the asymmetry between adversary operational tempo and annual or multi-year audit cycles; and (e) an audit-centric organizational culture that substitutes evidence production for risk reduction. The analysis situates these failures against a threat landscape defined by IT/OT convergence, industrial Internet of Things expansion, deep infrastructure interdependencies, nation-state pre-positioning, and ransomware economics. The paper then traces the intellectual and regulatory lineage of the alternative (continuous auditing, information security continuous monitoring, continuous diagnostics and mitigation, zero trust architecture, and emerging continuous control validation) and discusses implications for regulators, operators, and researchers. The compliance gap, it concludes, is not a maturity deficit but a design flaw requiring an architectural response. As a conceptual review the paper offers an analytic framework rather than an effect estimate: it presents no new data and does not establish that continuous regimes reduce realized risk relative to periodic ones, a limitation stated in full in Section 7.

KEYWORDS: critical infrastructure, audit-based compliance, continuous monitoring, configuration drift, NIST Cybersecurity Framework, operational technology security.

1. INTRODUCTION

Critical infrastructure constitutes the operational substrate of modern society. Electricity grids, water treatment plants, pipelines, hospitals, rail networks, and payment systems deliver services whose interruption propagates almost immediately into public safety, economic stability, and national security (Alcaraz & Zeadally, 2015; Rinaldi et al., 2001). Over the past two decades these systems have been progressively digitized: legacy operational technology (OT) has been coupled to enterprise information technology (IT), industrial processes have been instrumented with networked sensors, and supervisory control and data acquisition (SCADA) systems that were designed for isolated, trusted environments now exchange data with cloud platforms and remote maintenance channels (Igure et al., 2006; McLaughlin et al., 2016; Stouffer et al., 2023). The result is an attack surface that is larger, more dynamic, and more consequential than the one for which most cybersecurity governance regimes were designed (Humayed et al., 2017; Knowles et al., 2015).

Three characteristics distinguish critical infrastructure from ordinary enterprise computing and give the governance question its urgency. The first is consequence asymmetry: when an enterprise IT system fails, the loss is measured in data and money; when a control system fails, the loss can be measured in pressure, temperature, voltage, and ultimately in public harm. A misdirected actuator command is not an incident report; it is a physical event. The second is longevity. Industrial assets are procured on depreciation schedules of twenty to forty years, which means that devices designed before modern threat models existed will remain in service for decades to come, and that any assurance regime must govern a permanent mixture of old and new technology rather than a fleet that can be refreshed into safety. The third is coupling. CI systems are embedded in webs of physical and logical dependency: electricity feeds water treatment, telecommunications feeds grid telemetry, and all of them feed one another through shared suppliers, so the security state of any one operator is partly a function of decisions made elsewhere. Each of these characteristics interacts badly with an assurance instrument that observes a single organization, at a single moment, through the lens of its own documentation. The argument developed in this paper is, at bottom, an argument about that mismatch.

Against this backdrop, the dominant assurance instrument in critical infrastructure (CI) remains the periodic compliance audit. Whether conducted under the NIST Cybersecurity Framework (CSF), ISO/IEC 27001 certification, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards, or the European Union's NIS2 Directive, the underlying logic is similar: at defined intervals,

whether quarterly, annually, or triennially, an organization gathers evidence, an assessor evaluates that evidence against a control catalogue, and a verdict of conformance or nonconformance is rendered (European Parliament and Council of the European Union [NIS 2 Directive], 2022; International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2022a; National Institute of Standards and Technology [NIST], 2018; North American Electric Reliability Corporation [NERC], 2026). The audit produces a certificate, an authorization decision, or a regulatory filing, and the organization returns to normal operations until the next cycle.

Two terms should be fixed at the outset. "Audit-based compliance" here denotes any assurance regime whose primary verification events are scheduled and episodic, whether the assessor is an external certifier, a regulator, or an internal audit function; the argument is indifferent to who holds the clipboard. "Continuous control," by contrast, denotes a regime in which the existence, configuration, and effectiveness of security controls are observed and tested as an ongoing operational function, with assurance conclusions refreshed at the tempo of environmental change rather than at the tempo of the assessment calendar. The distinction is not between rigor and laxity, since a periodic audit can be exacting and a dashboard can be superficial, but between two different answers to the question of when the organization knows its own security state.

The central claim of this paper is that this model, however necessary as a governance baseline, is structurally incapable of ensuring real-time security in CI environments. The claim is not novel in its individual components: the accounting literature identified the obsolescence of periodic assurance for online systems more than three decades ago (Vasarhelyi & Halper, 1991); NIST formalized information security continuous monitoring (ISCM) as a federal expectation in 2011 (Dempsey et al., 2011); and practitioner surveys repeatedly document the gulf between certified compliance and operational resilience (Christopher, 2024; World Economic Forum [WEF], 2024). What has been lacking is a consolidated, theoretically grounded account of *why* audit-based models fail in CI specifically, and what the accumulated evidence implies for the design of successor regimes. This paper contributes such an account. It synthesizes standards documents, empirical OT security research, documented attack analyses, and the continuous auditing tradition into a structured argument organized around five failure modes of periodic compliance: static snapshots, manual process limitations, configuration drift, adversary speed, and audit-centric culture.

The paper proceeds as follows. Section 1.1 distinguishes what is claimed here from the closely related earlier work on which the argument depends. Section 2 characterizes the CI threat landscape that any assurance regime must now confront. Section 3 reconstructs the anatomy and regulatory context of audit-based compliance. Section 4 develops the five failure modes in detail. Section 5 assembles the case for continuous control, tracing its heritage in continuous auditing, its codification in ISCM and continuous diagnostics programs, and its extension through zero trust and continuous security validation. Section 6 discusses implications and the limits of the proposed remedy. Section 7 states the limitations of the study itself, and Section 8 concludes.

1.1 Relationship to Closely Related Prior Work

Because the argument below draws heavily on a connected body of recent work in operational technology assurance and continuous security validation, the boundary between what that work already established and what is claimed here should be stated explicitly rather than left for the reader to reconstruct from the citations. Four strands are close enough to the present thesis to warrant disclosure.

The first is the sector-specific work on electric utility operational technology. The systematic review of NERC CIP compliance in utility OT networks (Adegbite et al., 2020), together with the associated papers on IT and OT convergence architecture, ICS and SCADA detection, and vulnerability governance (Adegbite et al., 2022, 2023, 2024a), establishes for that sector that conformance is architected toward the audit boundary and that residual exposure persists in the intervals between assessments. That finding is an input to Section 4.3, not a result of it. The present paper does not re-derive it and does not claim the underlying sector evidence as its own contribution.

The second is the continuous security validation series (Dosunmu & Ogundele, 2024a, 2024c, 2024d, 2025a, 2025b), which develops breach-and-attack simulation and threat-informed defense engineering as operational disciplines and proposes their output as compliance evidence. Section 5.5 adopts that framing substantially intact. What is added here is not the validation stack but the claim that it is the functional successor to the periodic audit rather than a supplement to it, and the argument in Section 6.1 that it can only be deployed safely once earlier layers of the stack are in place.

The third is the continuous auditing tradition in accounting information systems (Alles et al., 2008; Chan & Vasarhelyi, 2011; Vasarhelyi & Halper, 1991; Vasarhelyi et al., 2012), which already contains both the general claim that assurance frequency must track transaction frequency and the evidence on adoption friction that Section 6.2 relies on. Section 5.2 transposes that literature into the security domain rather than extending it, and the transposition is an interpretive move whose limits are noted in Section 7.

The fourth is the normative continuous-monitoring literature itself: ISCM and its programmatic descendants (CISA, 2020; Dempsey et al., 2011, 2020) state the continuous expectation in official form and predate this paper by more than a decade. Section 5.3 reads those instruments as a sequence and draws an inference about regulatory direction from the sequence; it adds nothing to their content.

What remains as this paper's own contribution is correspondingly narrow, and it should be judged on that narrower basis. Three things are claimed. First, the consolidation of five separately documented weaknesses into a single dependency structure in which each mode aggravates the others, so that the aggregate failure is not the sum of the parts. Second, the argument that the resulting gap between documented and actual state is definitional rather than a maturity deficit, which is what distinguishes the diagnosis here from the large literature recommending that audits be performed better. Third, the sequencing and transition argument of Sections 6.1 and 6.2, which treats the continuous control stack as an ordered dependency graph rather than a menu. No new empirical data are presented, and none of the five failure modes is claimed as an original observation. Any authorship overlap between the present work and the studies named in this subsection is stated in the Declarations.

2. THE CRITICAL INFRASTRUCTURE THREAT LANDSCAPE

Any argument about assurance design must begin from the threat environment the assurance is meant to address. This section therefore characterizes the contemporary CI threat landscape along four dimensions: the technological convergence that has expanded the attack surface (Section 2.1), the interdependencies through which local failures become systemic ones (Section 2.2), the documented record of attacks on industrial systems (Section 2.3), and the differentiated actor landscape that generates those attacks (Section 2.4). The cumulative picture is of an

environment whose rate of change, technological, topological, and adversarial alike, is the central fact with which any assurance regime must contend.

2.1 IT/OT Convergence and the Expanding Attack Surface

The defining technological trend in CI over the past two decades is the convergence of information technology and operational technology. Industrial control systems (ICS), including SCADA masters, distributed control systems, programmable logic controllers, and remote terminal units, were historically isolated, proprietary, and protected primarily by obscurity and physical separation (Igure et al., 2006; Ralston et al., 2007). Economic pressure for real-time production data, remote maintenance, and predictive analytics has dissolved that separation, coupling control networks to corporate IT and, increasingly, to cloud services (McLaughlin et al., 2016; Stouffer et al., 2023). Each coupling point imports IT-class threats into environments where patching is constrained by availability requirements, device lifetimes are measured in decades, and safety consequences attach to security failures (Ani et al., 2017; Cárdenas et al., 2011; Kriaa et al., 2015).

The texture of this convergence is easiest to see in a concrete setting. Consider a mid-sized water treatment plant of the kind found in thousands of municipalities. Its filtration and dosing processes are governed by programmable logic controllers installed fifteen years ago; the controllers report to a SCADA server in a control room; the SCADA server exports production data to a corporate historian so that management can track chemical consumption; the historian is replicated to a cloud analytics platform under a contract signed by the finance department; an engineering workstation used to modify controller logic also receives email; and a maintenance contractor holds a remote-access account so that pump diagnostics can be run without a site visit. None of these couplings was introduced recklessly, since each solved a legitimate operational problem, yet together they compose a continuous path from the public internet to the chemical dosing logic. The security of the physical process now depends on the patch state of an email client, the credential hygiene of a third-party contractor, and the configuration of a cloud tenancy administered by people who have never seen the plant. An annual audit can, at best, verify that each coupling was documented and approved. What it cannot do is observe how the couplings behave in combination, day by day, as software is updated, accounts are created, and firewall exceptions are granted. The attack surface of the plant is not a list of assets; it is a constantly shifting graph of trust relationships, and the graph mutates far faster than any assessment calendar.

The Industrial Internet of Things (IIoT) intensifies this exposure. Networked sensors, actuators, and edge gateways multiply the number of addressable devices in industrial environments by orders of magnitude, many of them resource-constrained, unpatchable, and deployed with default credentials (Boyes et al., 2018; Sisinni et al., 2018). Sector reviews of IoT-enabled critical infrastructure make the same point for transportation and mobility systems, where safety-relevant functions increasingly depend on device populations that were never designed to be centrally governed (Jimoh et al., 2023a). The device layer itself is becoming harder to instrument. Research on radio-frequency energy harvesting for energy-autonomous sensing shows how far designers have gone to remove maintenance dependencies from deployed sensor populations (Asiedu & Quainoo, 2023a), and simulation of large-scale intermittently powered networks documents the reliability behavior of estates that are, by design, only sporadically available (Asiedu & Quainoo, 2023b); reliable broadcast protocols for batteryless intermittent sensor networks address the same condition at the communication layer (Asiedu & Quainoo, 2025). Devices of this kind are difficult to poll on an assessor's schedule and difficult to patch on any schedule at all. Systematic review of wireless system-on-chip testing shows how much functionality is now integrated into single, hard-to-inspect components (Quainoo & Ogundapo, 2026b), while models of Bluetooth and Wi-Fi coexistence in dual-mode devices (Quainoo & Ogundapo, 2026a), of impedance mismatch effects on link performance (Quainoo et al., 2024), and of throughput degradation in Wi-Fi 6 networks under varying channel conditions (Quainoo et al., 2025a) illustrate how much of a device's observable behavior depends on physical-layer conditions that no compliance artifact records. Smart grid modernization illustrates the pattern at sector scale: advanced metering, wide-area measurement, and demand-response systems create bidirectional communication paths that reach from consumer premises into transmission control, transforming the grid into a vast cyber-physical system whose integrity depends on the weakest of millions of endpoints (Mo et al., 2012; Wang & Lu, 2013). Reviews of smart grid architecture for high renewable penetration describe the same expansion from the operations side, as distributed generation, storage, and demand-side resources are absorbed into the control problem (Adenuga, 2022); comparative analyses of hierarchical, decentralized, and hybrid control architectures for distributed energy resources show that each topology distributes trust differently and therefore presents a different attack surface (Komi & Adamolekun, 2022); and edge intelligence approaches to microgrid control push decision authority outward to devices that periodic assessment rarely reaches (Komi & Ganiu, 2023). Assets that degrade continuously cannot be characterized adequately by inspection at intervals, whether the degradation is physical or configurational. Broader enterprise trends compound the effect: cloud migration relocates control-adjacent workloads onto shared infrastructure whose configuration is fluid by design (Ladapo et al., 2022b), while identity sprawl across hybrid and multi-cloud estates complicates the access governance on which OT segmentation depends (Mbonu et al., 2020a). Digital transformation of the surrounding supply chain compounds the effect by embedding IT risk and standards conformance obligations into operational workflows that previously sat outside the security perimeter (Mbonu et al., 2020b), and security architecture work on IT and OT convergence in regulated energy networks stresses that the governance model, not merely the network design, determines whether these couplings remain controllable (Adegbite et al., 2022). Taxonomies of SCADA attacks show that this expanded surface is exploitable at every layer, from field-device protocols to historian databases and engineering workstations (Zhu et al., 2011), and vulnerability assessments of power-system SCADA confirm that the consequences scale with the physical process under control (Ten et al., 2008). The observation burden that results is not confined to the cyber domain: energy operators increasingly instrument the physical layer as well, with national-scale unmanned aerial vehicle programs for power infrastructure inspection illustrating how heterogeneous the monitoring surface of modern grids has become: continuous physical asset surveillance now sits alongside cyber telemetry within the same governance perimeter (Dagodzo & Ahiaeke Patrick, 2025). The same logic appears in frameworks for integrating unmanned aerial inspection into national grid programs (Dagodzo, 2018) and in integrated aerial, LiDAR, and geospatial approaches to infrastructure corridor management (Dagodzo & Ahiaeke Patrick, 2021), both of which generate persistent observational streams about assets that regulatory inspection visits only occasionally.

2.2 Interdependency and Cascading Failure

CI sectors do not fail independently. Rinaldi et al. (2001) provided the canonical framework for infrastructure interdependency, distinguishing physical, cyber, geographic, and logical couplings through which disturbances propagate across sector boundaries; subsequent modeling work has confirmed that cyber interdependencies are among the least understood and most consequential (Ouyang, 2014). Electricity underpins water treatment, telecommunications, and healthcare; telecommunications underpins financial clearing and grid telemetry; and all sectors increasingly share common cloud, software, and hardware supply chains (Alcaraz & Zeadally, 2015; Okonkwo et al., 2024b). Resilience planning consequently treats supply chain continuity and infrastructure dependency as inseparable design problems, whether for gas processing plants embedded in national energy networks (Ogunwole et al., 2021) or for national diagnostic systems whose laboratory and logistics infrastructure must continue operating under public health stress conditions (Aminu-Ibrahim et al., 2025a). Supply chain risk models developed for engineering, procurement, and construction environments and for gas processing facilities treat disruption propagation as a primary design variable rather than a residual (Agbabiaka et al., 2019), and governance frameworks for digital supply chains in energy and infrastructure extend the same treatment to the data and platform layers through which operators are now coupled (Okonkwo et al., 2024a). Work on national-scale supply chain optimization through integrated IT and procurement systems shows how tightly the informational and physical layers are now bound (Okonkwo et al., 2025), while end-to-end visibility frameworks are explicitly motivated by the finding that transparency, compliance, and traceability fail together whenever visibility becomes intermittent (Nnabueze et al., 2021). Post-pandemic resilience indexing work makes the temporal point directly: resilience is a property that must be measured continuously, because it degrades between measurements (Efobi et al., 2023). The practical implication for assurance is severe: a control failure in one operator's environment is not contained by that operator's regulatory perimeter. Compliance regimes that certify organizations one at a time, on independent schedules, are poorly matched to risks that are systemic and temporally continuous (Linkov et al., 2013; WEF, 2025).

The temporal dimension of interdependency deserves particular emphasis, because it compounds the temporal weakness of periodic assurance. Cascading failures are fast: a protection relay misoperation propagates through a transmission network in seconds, a telecommunications outage severs utility telemetry within minutes, and the operational decisions that determine whether a disturbance is contained or amplified are made in the first hour. Audit findings, by contrast, are reconciled across organizations over months, if at all. There is no mechanism by which one operator's discovery of a compromised vendor or a poisoned software update propagates through the compliance system to the hundreds of other operators exposed to the same dependency; each will discover the issue at its own next assessment, or through an incident. Interdependent infrastructure therefore needs not merely continuous monitoring within each operator but timely propagation of security state across operators, a requirement that the one-organization-at-a-time audit model cannot express, let alone satisfy.

2.3 Documented Attacks on Industrial Systems

The empirical record removes any doubt that these exposures are actively exploited, although what the record establishes and what is sometimes inferred from it should be kept apart. Stuxnet demonstrated in 2010 that a sophisticated actor could cross an isolated network boundary, subvert programmable logic controllers, replay recorded process values so that operator displays showed normal readings, and physically damage industrial equipment (Falliere et al., 2011; Langner, 2011). The technical analyses establish the tradecraft in detail; they do not describe the target facility's assurance arrangements, and no claim is made here about what an audit of that facility would have found. The December 2015 attack on the Ukrainian power grid taught a complementary lesson: adversaries conducted months of patient reconnaissance, harvested credentials, and then synchronized breaker operations, firmware corruption, and telephony denial-of-service to blind and delay response, all within distribution utilities operating under national regulatory oversight, though the public analysis characterizes the intrusion rather than the specific assurance regime those utilities were subject to (Lee et al., 2016). More recently, joint advisories have documented the "Volt Typhoon" campaign, in which People's Republic of China state-sponsored actors used living-off-the-land techniques, that is, native administrative tools rather than malware, to establish persistent, pre-positioned access inside U.S. communications, energy, transportation, and water infrastructure while generating few of the file-based artifacts on which signature detection and document-centric review typically rely (Cybersecurity and Infrastructure Security Agency [CISA], 2023a; CISA, 2024). The advisories report technique and prevalence; they do not report the compliance status of the affected entities. Systematic reviews of machine-learning-based anomaly detection for industrial control systems exist precisely because behavioral traces, rather than file artifacts, are what remains observable in such campaigns (Adebayo et al., 2023), and detailed catalogues of directory service attack steps and signatures show how much modern intrusion tradecraft consists of legitimate administrative operations executed by an illegitimate principal (Ladapo et al., 2023). Vulnerability governance architectures developed for power and utility corporations respond to the same problem by tracking exposures from mapping through remediation verification rather than certifying their absence at a point in time (Adegbite et al., 2024a).

Industry telemetry corroborates the trend lines. Dragos (2025) reports sustained growth in ICS-capable threat groups and ransomware incidents affecting industrial operators; Fortinet (2024) finds that a majority of industrial organizations experienced intrusions that reached their OT systems; and Claroty (2024) documents the material business impact of cyber-physical disruptions, including recovery costs and operational downtime concentrated in exactly the sectors regulators designate as critical. Cross-sector breach analyses show attackers exploiting unpatched edge devices and stolen credentials at scale, with exploitation of vulnerabilities as an initial access vector growing sharply year over year (Verizon, 2024, 2025). The financial exposure is substantial and persistent, with average breach costs in critical sectors well above cross-industry means (IBM, 2024, 2025).

Read together, these cases suggest a common analytical lesson for assurance design, though it must be stated with more care than it usually receives. What the public record establishes in each instance is that an adversary operated for an extended period inside an environment whose defenders did not detect the operation. What the record does not establish, in any of the three, is the state of the victim's formal compliance posture at the time: certification status, audit findings, and control-testing results for these organizations are not in the public domain, and claims that the victims were "certified but compromised" are therefore assertions rather than findings. The defensible lesson concerns the object of organizational knowledge. In each case what proved decisive was the operator's awareness of its own live state: Stuxnet's implant replayed recorded process data to the systems on which that awareness depended (Falliere et al., 2011); the Ukrainian attackers spent months inside the environment, learning it

more thoroughly than its defenders monitored it (Lee et al., 2016); and Volt Typhoon's tradecraft was selected to minimize the artifacts that retrospective, document-centric review examines (CISA, 2023a, 2024). In that limited sense the incidents exploited the interval during which documented state and actual state diverge. The stronger claim advanced in this paper, that an assurance model verifying documents at intervals does not merely fail to close that interval but institutionally defines it, does not follow from three cases. It is developed in Section 4 from the structure of the assurance model itself, and these incidents illustrate the argument rather than establish it.

2.4 Threat Actors: Nation-States, Ransomware Economies, and Insiders

The actor landscape facing CI is differentiated and professionalized. At the high end, nation-state and state-affiliated groups conduct long-horizon campaigns whose objective is not immediate monetization but strategic pre-positioning, with access maintained quietly for potential disruption during geopolitical crisis (CISA, 2023a, 2024; European Union Agency for Cybersecurity [ENISA], 2024). Structured threat-actor analysis has therefore become a planning discipline in its own right, linking actor capability and intent to enterprise defensive priorities (Dosunmu & Ogundele, 2023). At the volume end, ransomware has evolved into a mature criminal economy with affiliate models, initial-access brokers, and double-extortion tactics; hospitals and utilities are attractive targets precisely because service interruption creates immediate pressure to pay (ENISA, 2023; Ozowara et al., 2025). Availability attacks require no such economics at all: protocol-level amplification allows a small number of hosts to generate service-denying traffic volumes, and mitigation depends on continuously maintained network configuration rather than on any periodic attestation (Jimoh & Ahmed, 2024). Empirical reviews link the resulting losses directly to organizational financial performance, making cyber risk a board-level solvency issue rather than a technical externality (Ozowara et al., 2022). Insider threats add a third dimension: privileged users whose misuse or compromise bypasses perimeter controls entirely and whose behavior is invisible to document-based audits (Akeju et al., 2018). Studies of security awareness training and insider-threat behavior in administrative populations find that measured behavioral change, rather than training completion records, is the variable that matters (Onche et al., 2024), and capability frameworks for human factors in information security make the same argument at the level of role design (Onche et al., 2026). The division of labor within the ransomware economy is itself a tempo problem: because initial access, monetization, and negotiation are performed by different specialists, an exposed credential or unpatched appliance can be sold and weaponized by parties who incurred none of the cost of discovering it, and the interval between exposure and exploitation is set by a market rather than by any single actor's capacity. Defensive regimes that implicitly assume a slow, unitary adversary therefore misprice the risk of every transient weakness.

Two features of this landscape bear directly on assurance design. First, adversary tradecraft is now systematically catalogued, since the MITRE ATT&CK knowledge base and its ICS extension enumerate hundreds of techniques observed in real intrusions, which means defenders can, in principle, test controls against realistic behavior rather than abstract requirements (Alexander et al., 2020; Strom et al., 2020). Integrated threat intelligence automation and simulation models operationalize this by feeding catalogued technique data continuously into defensive testing (Dosunmu & Ogundele, 2026b), and deception-based architectures go further by instrumenting the environment so that adversary presence generates signal rather than silence (Dosunmu & Ogundele, 2026a). Second, the tempo of exploitation has collapsed: known exploited vulnerabilities are weaponized within days of disclosure, which is why U.S. authorities now maintain a living catalogue with binding remediation deadlines measured in weeks rather than audit cycles (CISA, n.d.a). An assurance model built for this landscape must operate on the adversary's clock, not the auditor's. Surveys of enterprise threat evolution reach the same conclusion: the attack surface and the actor set are both changing faster than annual governance instruments can register (ENISA, 2024; Okoruwa et al., 2024).

3. ANATOMY OF AUDIT-BASED COMPLIANCE

3.1 The Logic and Lifecycle of the Periodic Audit

Audit-based compliance rests on a defensible chain of reasoning: risks are identified and assessed; controls are selected to mitigate them; and an independent party periodically verifies that the controls exist and operate as designed. The chain is codified in the major risk management standards. NIST's Risk Management Framework structures the lifecycle as categorize, select, implement, assess, authorize, and monitor (Joint Task Force, 2018), with control catalogues and assessment procedures specified in companion volumes (Joint Task Force, 2020, 2022). Risk assessment methodology is elaborated in dedicated guidance (Joint Task Force Transformation Initiative, 2011, 2012), and parallel structures exist in the ISO ecosystem, where ISO/IEC 27001 defines the information security management system subject to certification audit, supported by risk management guidance in ISO/IEC 27005 and the general risk framework of ISO 31000 (International Organization for Standardization [ISO], 2018; ISO/IEC, 2022a, 2022b). Enterprise risk frameworks such as COSO extend the same periodic-review logic to organizational governance broadly (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017), and NIST's own guidance on integrating cybersecurity with enterprise risk management inherits it (Stine et al., 2020).

In practice, the audit lifecycle in CI unfolds as an episodic campaign. Months before the assessment, the organization assembles evidence: policy documents, network diagrams, access reviews, vulnerability scan reports, training records. Assessors then sample this evidence, conduct interviews, and test a subset of controls, producing findings and a plan of actions and milestones. Between campaigns, formal verification activity largely ceases. Security audit and enterprise risk assessment frameworks in the practitioner literature describe exactly this cadence, along with its known weaknesses in coverage and timeliness (Dosunmu & Ogundele, 2019; Fadayomi et al., 2019). The internal audit literature describes the same lifecycle from the assurance provider's side, including efforts to raise audit quality through technology-enabled risk assessment (Akomolafe & Agu, 2018) and to reorient engagement planning around risk rather than checklist coverage (Akomolafe et al., 2023). Comparative work on SOX compliance frameworks in cross-border settings shows how the cadence hardens once statutory reporting deadlines anchor it (Agu et al., 2023), and studies of audit liaison and corrective action planning in multinational organizations document the substantial administrative apparatus that accumulates around the finding-and-remediation cycle (Ebhojie et al., 2023). Physical asset assurance offers an instructive parallel, because it faces the same inspection-interval problem in a domain where the degradation mechanism is well understood. Inspection there is scheduled, sampled, and extrapolated across the interval between campaigns, exactly as control testing is. The response in that field has not been to abandon inspection but to supplement it with continuously collected condition data, for reasons that Section 4 develops in the security case. Even

sophisticated technical assessments are typically conducted offline, against exported configurations or lab replicas, precisely because assessing live safety-critical systems is operationally hazardous, an accommodation that further widens the gap between the assessed artifact and the running system (Ladapo et al., 2018).

It is instructive to walk through what the assessor actually sees. Suppose the auditor of a combined-cycle power plant requests evidence for a network segmentation requirement. The operator supplies a firewall rule export taken on the day the evidence package was assembled, a network diagram last revised during a control system upgrade two years earlier, and a change-management log. The auditor samples perhaps twenty-five rules from a rulebase of three thousand, checks them against the diagram, interviews the network engineer about the exception process, and concludes that the control is designed and operating effectively. Every step of this procedure is professionally sound, and every step measures something other than the live network. The rule export is a text file, not the running configuration: it does not reveal the temporary any-to-any rule inserted during last month's historian migration and scheduled, informally, for removal. The diagram describes the intended topology, not the maintenance laptop currently bridging two zones. The interview elicits the process as the engineer understands it, not the process as enacted at two in the morning during an outage. The sampled rules are, by construction, the ones that exist in the export; the audit has no procedure for observing traffic that flows in violation of the ruleset through paths the ruleset does not describe. None of this reflects negligence. It reflects the epistemology of the audit: an inference from curated artifacts to operational reality, performed at a single point in time. The inference is only as good as the correspondence between artifact and reality, and it is exactly that correspondence that modern, high-churn environments continuously erode.

3.2 The Regulatory Context

The regulatory architecture surrounding CI institutionalizes this cadence, though the instruments differ more than the common label suggests, and the difference matters because it determines where the periodicity actually originates. The NIST CSF, first released in 2014, revised as version 1.1 in 2018 and as version 2.0 in 2024, organizes cybersecurity outcomes into functions: Identify, Protect, Detect, Respond, Recover, and, from version 2.0, Govern (NIST, 2018, 2024). Three qualifications should be attached to it before it is enlisted as an example of periodic assurance. First, the CSF is voluntary guidance rather than a compliance standard: it confers no certification, designates no assessor, and creates no obligation except where a separate contract, regulation, or procurement condition incorporates it. Second, version 2.0 broadened the framework's stated audience beyond critical infrastructure to organizations of any sector or size, so its status as a CI instrument is now a matter of adoption rather than of scope. Third, and most importantly for the argument developed here, the framework does not prescribe assessment frequency, and in places points the other way: the Continuous Monitoring category within the Detect function, and the Improvement category introduced in version 2.0, describe standing capabilities rather than scheduled events. The periodicity, in other words, is not in the text. It enters through implementation, where organizations operationalize the framework as current-and-target profile comparisons and maturity scores produced on an annual or biennial cadence, and the measurement literature finds that most CSF-based assessment in practice reduces to point-in-time scoring (Gordon et al., 2020; Krumay et al., 2018). The CSF is accordingly better read as permitting continuous assurance than as obstructing it. What obstructs it is the assessment practice that has accumulated around the framework, which is a different object and requires a different remedy.

Sector-specific and jurisdictional regimes add enforcement teeth, and here the periodic form is in the instrument rather than merely in its implementation, though with qualifications that are usually elided. NERC CIP subjects North American bulk electric system operators to mandatory, audited requirements, and it is risk-tiered rather than uniform: obligations attach according to whether a BES Cyber System is categorized as high, medium, or low impact, so the most demanding controls reach only part of the registered estate while low-impact assets carry a substantially reduced requirement set. Verification runs through the ERO Enterprise's Compliance Monitoring and Enforcement Program, which combines full compliance audits at risk-based intervals commonly cited as three to six years with self-certifications, spot checks, self-reports, and investigations in the intervening periods. The standards development process itself runs on multi-year cycles that the regulator's own roadmap acknowledges must accelerate (NERC, 2026). Systematic review of NERC CIP compliance in electric utility operational technology networks finds the expected pattern: conformance is architected for, and demonstrated at, the audit boundary, while the residual threat surface remains architectural and persistent (Adegbite et al., 2020).

The approval of CIP-015-1 on internal network security monitoring is best read as a partial regulatory concession that perimeter-focused, periodically verified compliance is insufficient. Its scope and timing should be stated precisely, however, because both are frequently overstated in the commentary. FERC approved the standard in Order No. 907 in June 2025, with an effective date in September 2025 (CIP-015-1, 2025). The obligation reaches all high-impact BES Cyber Systems and medium-impact systems with external routable connectivity; low-impact systems fall outside it. Compliance is phased, with control centers required to conform thirty-six months after the effective date and the remaining applicable systems sixty months after, placing full effect in 2028 and 2030 respectively. FERC further directed NERC to extend coverage to electronic access control or monitoring systems and physical access control systems located outside the electronic security perimeter. The direction of regulatory travel is therefore unambiguous, but at the time of writing continuous internal monitoring is an approved future obligation covering part of one sector, not a present requirement across critical infrastructure, and arguments that treat it as the latter overstate the current state of the law.

In Europe, the NIS2 Directive substantially expands the population of regulated entities and, through Article 20, places cybersecurity risk management under the approval and oversight of management bodies with personal accountability attached (NIS 2 Directive, 2022). Its supervisory model is two-tiered rather than uniformly periodic, and the distinction bears on the argument of this paper. Essential entities are subject to ex ante supervision under Article 32, which authorizes on-site inspections and random checks, regular and targeted security audits carried out by an independent body or competent authority, ad hoc audits where justified by a significant incident, and security scans. Important entities are subject to ex post supervision under Article 33, triggered by evidence or indication of non-compliance rather than exercised on a schedule. NIS2 therefore does not simply institute an annual audit: for the larger tier it authorizes a mixture of scheduled and unscheduled verification, and for the smaller tier it substitutes reactive supervision for scheduled verification altogether. What it retains in both tiers is verification by inspection of an entity at discrete moments, and it is that property, rather than any particular cadence, on which the present argument turns. Implementation is also uneven. Transposition was due by 17 October 2024 and was completed on time by only a minority of Member States, and ENISA's maturity analysis of NIS2 sectors finds wide variance in readiness, with several critical sectors falling below baseline (ENISA, 2025).

Beyond the two flagship regimes, a wider family of instruments shares the same verification architecture. Complementary instruments, among them the U.K. Cyber Assessment Framework, the U.S. cross-sector performance goals, CMMC for the defense industrial base, and the protection requirements for controlled unclassified information, likewise define what must be true of an environment, verified at assessment time (CISA, 2023b; National Cyber Security Centre [NCSC], 2024; Ross & Pillitteri, 2024; U.S. Department of Defense, Office of the Chief Information Officer [U.S. Department of Defense], 2024). Financial-sector compliance frameworks follow the same audited-control pattern (Bello et al., 2024), as do the IT general control regimes descended from financial reporting law (Mbonu et al., 2022a). Comparable structures govern data protection across jurisdictions, where obligations are specified as implementable controls and verified through periodic assessment (Mbonu et al., 2019a), and pharmaceutical regulation exhibits the same architecture in another high-consequence sector, whether in cross-border harmonization models for market authorization (Eze et al., 2024) or in supplier risk assessment regimes for international procurement (Akin-Oluyomi et al., 2023). Procurement compliance in high-risk energy environments is likewise organized around documented conformance at defined checkpoints (Okonkwo et al., 2021). Reviews of the role of frameworks in cybersecurity governance identify the underlying tension directly: frameworks coordinate expectations effectively while specifying outcomes loosely enough to be verified by inspection (Jimoh et al., 2023b).

The periodic-certification pattern, and its limits, are not unique to cybersecurity regulation. Civil aviation, itself a regulated critical infrastructure sector, has long anchored oversight in aerodrome certification and scheduled safety audits, and comparative studies show both that certification compliance can be benchmarked across regulators (Adeyelu & Dagodzo, 2022) and that audit outcomes are substantially predictable from organizational maturity characteristics observable well before the audit event itself (Adeyelu & Dagodzo, 2024), evidence that the audit often confirms, rather than discovers, the state of the system. The sector's regulatory response has been the safety management system: an adaptive, continuously operating assurance process embedded in daily operations rather than a certification event (Adeyelu, 2019), complemented by predictive compliance monitoring that mines continuously accumulating operational data, such as consumer complaint streams, for systemic safety risks between formal audits (Adeyelu, 2018). Aviation's trajectory thus prefigures the argument developed in Section 5: certification-based oversight in high-hazard domains tends, under the pressure of operational experience, toward continuous and data-driven supervision.

3.3 What Audits Do Well

A fair assessment must acknowledge the genuine functions of periodic audit. Audits create accountability structures and board visibility that purely technical operations lack (Posthumus & von Solms, 2004); they force the documentation and inventory work that is a precondition for any security program (von Solms & von Solms, 2004); they harmonize expectations across supply chains; and certification signals, imperfect as they are, reduce information asymmetry between operators, regulators, insurers, and customers, and can even function as competitive differentiators (Annan, 2025; Culot et al., 2021). Comprehensive financial reporting models make the analogous case in their own domain, treating disciplined reporting as the mechanism through which accountability becomes enforceable rather than aspirational (Medon & Oduleye, 2022), and governance and accountability models for public-private partnerships in infrastructure show why an inspectable record matters most precisely where responsibility is shared across organizations (Aminu-Ibrahim et al., 2024). Work on data-driven compliance analytics in financial institutions indicates how this legitimate function can be preserved without the periodic form, by grounding governance conclusions in continuously collected evidence (Akomolafe et al., 2025). These functions are real, and any successor regime must preserve them: boards will still need attestations they can rely on, procurement will still need comparable signals of supplier hygiene, and regulators will still need defensible enforcement records. The correct conclusion is therefore not that periodic verification is worthless but that it answers a narrower question than the one CI protection actually poses. An audit answers the question of whether the organization was able to demonstrate its controls at a given moment; security requires an answer to whether the controls are working now. The two questions coincide only in a static world. The argument of this paper is accordingly not that audits should be abolished, but that they were never designed to provide, and cannot provide, the real-time assurance that CI now requires. The failure modes examined next explain why.

4. FIVE FAILURE MODES OF PERIODIC COMPLIANCE

The five failure modes developed in this section are analytically distinct but operationally entangled. The first two concern what an audit can know: the snapshot problem limits when knowledge is acquired, and manual process limitations constrain how much can be known at all. The third and fourth concern what happens between audits: the environment drifts away from its certified state, and adversaries move through the resulting gaps at a tempo no assessment calendar can match. The fifth concerns what the audit regime does, over time, to the organization that lives under it. Each is documented independently in the literature; their joint effect is the compliance gap.

4.1 Failure Mode 1: The Static Snapshot

The foundational defect of audit-based assurance is temporal. An audit is a measurement of system state at time t; its verdict is then treated, implicitly, as valid over the interval [t, t + cycle length]. This inference is sound only if the environment is approximately stationary over the interval, an assumption that held tolerably for the batch-processing systems of early computing and fails completely for modern CI estates characterized by continuous configuration change, workload migration, credential churn, and device turnover (Stouffer et al., 2023; Vasarhelyi & Halper, 1991). The audit certificate is thus a claim about the past presented as a claim about the present.

The measurement literature has long warned about precisely this category error. Security is notoriously difficult to measure even instantaneously, because it is a property of the interaction between a system and an adaptive adversary rather than of the system alone (Pfleeger & Cunningham, 2010); metrics regimes that reward the production of favorable point-in-time indicators invite gaming and provide weak evidence of protection (Jaquith, 2007). Under conditions of genuine uncertainty, where the probability distributions of adversary behavior are themselves unknown, point estimates are especially fragile as a basis for decisions (Knight, 1921). The practical consequence in CI is a structural visibility gap: misconfigurations, unauthorized changes, and control failures arising the day after an assessment remain formally invisible until the next one, a window that documented intrusions show adversaries exploiting deliberately (CISA, 2024; Lee et al., 2016). Stuxnet is the limiting case: the victim environment would have passed contemporaneous compliance review while its centrifuge controllers executed sabotage logic and reported fabricated telemetry (Falliere et al., 2011; Langner, 2011).

It is worth being precise about how the snapshot's validity decays. On the day after the assessment, the certificate's claim and the environment's state differ by whatever changed overnight, typically little. But change accumulates multiplicatively across interacting components: each new account, rule, device, and software version alters the context in which every existing control operates, so the divergence between certified state and actual state grows not additively but combinatorially. By the midpoint of an annual cycle, the certified description and the operational environment may share little more than a topology. Crucially, the organization has no instrument for knowing where in this decay curve it currently sits: the audit regime measures position only at the endpoints of the interval, never within it. The result is a peculiar epistemic rhythm, familiar to practitioners, in which organizational confidence about security state peaks immediately after each assessment and then degrades, invisibly and unmeasurably, until the next evidence-gathering campaign forcibly re-synchronizes the paperwork with reality. Adversaries face no such rhythm; their knowledge of the environment is refreshed by every packet they observe. The contrast with adjacent management disciplines is instructive. Real-time performance indicator tracking is now routine in operational and financial management, where automated monitoring has largely displaced periodic reporting as the basis for decisions (Tonoyan et al., 2024b), and executive dashboards deliver continuously refreshed financial state to the same boards that accept annual attestations about security state (Walawalkar et al., 2025). Industrial safety made the equivalent move earlier still, through proactive hazard recognition and near-miss reporting systems designed to surface conditions before they become events (Obogo et al., 2021). Cybersecurity assurance in critical infrastructure is conspicuous chiefly for having retained the older cadence.

4.2 Failure Mode 2: Manual Process Limitations

Periodic audits are labor-intensive artifacts of human judgment: evidence is requested, assembled, sampled, and interpreted by people working against deadlines. Three well-documented limitations follow. First, sampling: assessors examine a fraction of systems, accounts, and rules, and extrapolate; in heterogeneous OT/IT estates with thousands of devices and firewall rules, the sampled fraction shrinks toward statistical irrelevance (Knowles et al., 2015). Second, interpretation variance: control requirements are expressed in natural language, and studies of risk assessment practice show wide methodological divergence in how nominally identical requirements are evaluated, to the point that the field has been described as a "maze" of incommensurable methods (Cherdantseva et al., 2016; Gritzalis et al., 2018). Third, fatigue and error: evidence collection is repetitive clerical work performed under time pressure, and the general human-factors literature on monitoring and verification tasks documents systematic degradation in vigilance and accuracy under exactly these conditions (Parasuraman & Manzey, 2010). Human error causation research in high-hazard industrial settings reaches the same conclusion about verification tasks performed under schedule pressure, and locates the cause in task design rather than in individual diligence (Obriki & Arumosoye, 2020).

The arithmetic of sampling deserves a moment of attention, because its implications are routinely underestimated. An assessor who examines twenty-five of three thousand firewall rules has observed less than one percent of the control surface; if even a handful of rules are misconfigured, the probability that a small random sample contains none of them is high, and the audit will conclude, correctly by its own procedure but wrongly in fact, that the control operates effectively. The problem worsens as estates grow: the sample size is fixed by assessor time, while the population grows with every device, account, and rule added to the environment, so proportional coverage declines monotonically even when audit effort is held constant. Sampling theory, moreover, presumes that defects are distributed randomly, whereas security-relevant defects matter adversarially precisely when they are rare and unrepresentative: the one orphaned administrator account matters more than the thousand well-managed ones. Statistical assurance techniques built for detecting systemic error rates in financial transactions transfer poorly to a domain in which a single exceptional item can constitute the entire loss event. Automation has been the standard response to the clerical component of this problem elsewhere: process automation frameworks in procurement were adopted precisely to remove manual handling from high-volume verification work (Akinleye & Adeyoyin, 2021), and embedded automated close controls in public sector enterprise resource planning systems convert audit readiness from a periodic assembly exercise into a continuously maintained property of the system (Oyeleye et al., 2025). Software engineering offers the closest analogue, in which automated regression and security testing displaced manual inspection as the primary verification mechanism for changing systems long ago (Mbonu et al., 2021), and reviews of test automation in wireless hardware engineering document the same displacement of manual, instrument-driven verification by scripted and repeatable execution (Quainoo et al., 2025b).

The workforce context aggravates all three. Cybersecurity skills shortages are persistent and most acute in the OT specializations that CI audits require (Dawson & Thomson, 2018; Furnell, 2017). Scarce experts spend audit season producing documentation rather than reducing risk, an opportunity cost that practitioner surveys of ICS security programs identify as material (Christopher, 2024). Moreover, manual assessment simply cannot inspect what matters most in modern environments: infrastructure defined in code, ephemeral cloud workloads, and machine-speed access decisions. Empirical analysis of infrastructure-as-code repositories finds security "smells" such as hard-coded secrets, permissive defaults, and suspect configurations to be pervasive at rates no manual review process could feasibly detect (Rahman et al., 2019), which is why governance proposals for code-defined infrastructure converge on automated, pipeline-embedded checking rather than human review (Mbonu et al., 2020c).

4.3 Failure Mode 3: Configuration Drift

Even a perfectly executed audit of a perfectly compliant environment begins to lose validity immediately, because the environment moves. Configuration drift, the gradual, cumulative divergence of running systems from their approved baseline, is driven by routine operations: emergency changes made under time pressure and never reverted, firewall exceptions granted for maintenance vendors, software updates that reset hardened settings, and access rights that accrete as roles change but are never revoked (Soomro et al., 2016; Stouffer et al., 2023). In cloud-integrated estates the drift rate is higher still, because configuration is programmable and change is continuous; misconfiguration of cloud resources has accordingly emerged as a leading cause of exposure, motivating dedicated continuous misconfiguration-monitoring frameworks (Aliliele et al., 2023; Torkura et al., 2021). Identity is a particularly corrosive drift vector: reviews of identity and access management in hybrid environments document how entitlement sprawl across directories and cloud platforms defeats the least-privilege assumptions on which audited access controls rest (Mbonu et al., 2020a), and long-lived directory infrastructures accumulate exactly the stale, over-privileged objects that offline assessments later struggle to untangle (Ladapo et al., 2018). Work on cloud identity and access governance in large enterprise estates documents the accretion mechanism in detail and treats entitlement review as a continuous optimization problem rather than an annual campaign (Mbonu et al., 2022b),

while operational studies of directory service implementation show how quickly administrative convenience produces durable privilege structures that no one subsequently owns (Ladapo et al., 2019).

A concrete chronology shows how quickly the certified state dissolves. Consider an OT/IT hybrid manufacturing plant audited, successfully, in January. In February, a controller fault requires an emergency firmware rollback; the replacement image predates the hardening guide, and the deviation is logged for correction "when production allows." In March, a vendor needs remote access to retune a compressor; a firewall exception is opened for the engagement and, because the vendor's follow-up visit keeps being rescheduled, never closed. In April, the enterprise IT department migrates the historian to a cloud service, and a synchronization agent is installed inside the control network with credentials stored in a configuration file. In May, an engineer leaves; his account is disabled in the corporate directory but survives on three OT servers that authenticate locally. In June, an operating system update on the engineering workstation silently re-enables a legacy file-sharing protocol that the January baseline had disabled. None of these events is an incident. None violates policy in a way anyone notices. Several were individually approved. Yet by midsummer the plant differs from its certified configuration in at least five security-relevant respects, each of which enlarges the attack surface, and the compliance apparatus is not merely unaware of the specifics; it is structurally incapable of becoming aware of them before the next assessment, which is seven months away. Multiply this chronology across hundreds of systems and dozens of teams, and the certified environment becomes an increasingly fictional object, maintained in documentation and nowhere else. Data estates drift in the same way and for the same reasons: governance architectures for enterprise data platforms are motivated by the observation that classification, retention, and access controls degrade silently as pipelines are added (Aliliele et al., 2025b), and sensitivity classification frameworks with regulatory traceability exist because the mapping between data, its handling requirements, and its actual location must be maintained rather than merely established (Aliliele et al., 2024a). Maintenance engineering reached the analogous conclusion about physical assets decades ago, in the shift from reactive to predictive regimes grounded in continuous condition data (Sunday et al., 2020). The parallel with physical asset management is more than rhetorical: reliability-centered maintenance practice in high-density computing environments schedules intervention against observed condition precisely because time-based assumptions fail once utilization varies (Oyeleke et al., 2026).

Drift matters because attackers consume it. Breach investigations consistently trace intrusions to exposures that postdate the victim's last assessment: an unpatched edge appliance, a re-enabled legacy protocol, an orphaned account with a weak credential (Verizon, 2024, 2025). Living-off-the-land tradecraft is, in essence, the weaponization of drift, since adversaries operate through legitimate tools and accumulated misconfigurations precisely because these leave no malware for defenders to find (CISA, 2023a). The audit model has no mechanism for observing drift as it occurs; it can only discover, at the next cycle, that the certified state no longer exists. Chaos-engineering research makes the point constructively: when experimenters deliberately inject configuration faults into cloud infrastructure, conventional periodic assurance detects almost none of them, whereas continuous automated detection identifies and remediates the majority (Torkura et al., 2020).

4.4 Failure Mode 4: Adversary Speed Versus Audit Cycles

The fourth failure mode is an arithmetic mismatch between offensive and assurance tempos. Contemporary intrusion campaigns compress reconnaissance, initial access, privilege escalation, and lateral movement into days or hours; ransomware operations in particular have industrialized this pipeline through access brokers and affiliate specialization (ENISA, 2023, 2024). Vulnerability exploitation timelines have shortened to the point that national authorities mandate remediation of known exploited vulnerabilities within weeks (CISA, n.d.a) and issue standing "shields up" postures during periods of elevated threat (CISA, n.d.b). Meanwhile the assurance cycle in CI runs at annual or multi-year periods, and the regulatory standards development cycle runs slower still (NERC, 2026). An adversary who gains access the week after an audit enjoys, in the median CI environment, months of formally unexamined dwell time.

The asymmetry can be stated numerically. If exploitation of a newly disclosed vulnerability begins within days (CISA, n.d.a) and a typical CI assessment cycle runs twelve months, the defender's formal verification frequency is slower than the adversary's opportunity frequency by roughly two orders of magnitude. Even quarterly assessment, rare in practice because of its cost in scarce expertise, leaves a window of about ninety days, which is more than an order of magnitude longer than the interval modern intrusion campaigns need to progress from initial access to operational objectives. The point is not that faster audits would close the gap; no feasible audit cadence approaches the required tempo. The point is that cadence itself is the wrong variable. A verification event, however frequent, samples the contest; only a verification process participates in it.

Detection research quantifies the cost of this asymmetry. The intrusion detection tradition beginning with Denning (1987) exists precisely because prevention and periodic verification cannot be assumed effective; four decades of subsequent work on anomaly and misuse detection is, collectively, an argument that security-relevant events must be observed as they happen or not at all (Ahmed et al., 2016; Bhuyan et al., 2014; Chandola et al., 2009; García-Teodoro et al., 2009). Intrusion detection and prevention models developed for enterprise defense make the operational version of this argument, treating continuous inspection as the only control that acts within the adversary's timeframe (Dosunmu & Ogundele, 2020), and security operations architectures designed for utility-sector centers integrate threat intelligence, behavioral analytics, and automated response for the same reason (Adegbite et al., 2024b). Attack modeling frameworks reinforce the point: ATT&CK-style technique chains unfold as sequences of small, individually ambiguous actions whose recognition requires correlating telemetry across the whole chain in near real time (Strom et al., 2020), and projection research shows that meaningful forecasting of attack progression is only possible on continuous data streams (Husák et al., 2019). Threat intelligence integration frameworks likewise presuppose an operational tempo of hours, not quarters: indicators age out long before any audit could act on them (Dosunmu & Ogundele, 2022). Control validation faces the same clock: breach simulation methods applied to firewalls and endpoint defenses are designed to test enforcement points repeatedly, because a configuration verified once is verified only for that configuration (Dosunmu & Ogundele, 2026c). Financial monitoring offers an instructive parallel, where anomaly detection over transaction time series is assumed to operate continuously because the exposure it addresses is continuous (Atakpa & Fobellah, 2023). Incident response doctrine has internalized the same reality, treating rapid detection-to-containment intervals as the primary controllable determinant of impact (Dosunmu & Ogundele, 2021; Nelson et al., 2025). No assessment schedule, however diligent, participates in this contest; audits are simply not on the field when the engagement occurs.

4.5 Failure Mode 5: Audit-Centric Culture and the Substitution of Compliance for Security

The final failure mode is organizational rather than technical. When regulatory consequences attach to audit outcomes rather than security outcomes, rational organizations optimize for the former. The behavioral information security literature documents the mechanism: compliance behavior responds to perceived sanction, cost, and normative pressure, not to underlying risk (Bulgurcu et al., 2010; Safa et al., 2016), and security culture research shows that what leadership measures and rewards becomes what the organization values (AlHogail, 2015). The safety literature has developed this point furthest, in leadership models linking managerial attention to safety culture formation (Obogo et al., 2023) and in accounts of culture transformation across large workforces where the observable driver is what supervisors attend to daily rather than what the policy states (Obogo et al., 2019). Under an audit-centric regime, the measured artifact is evidence, whether policies, attestations, or screenshots, so evidence production becomes the de facto security program. Von Solms and von Solms (2004) list precisely this substitution of policy documents for operational practice among the "deadly sins" of information security management, and governance scholarship has repeatedly warned that compliance and security are related but distinct objectives that diverge under pressure (Posthumus & von Solms, 2004; von Solms & van Niekerk, 2013).

The economics of the substitution are intelligible. Security investment is subject to diminishing returns and severe measurement difficulty (Gordon & Loeb, 2002); when the observable payoff is a passed audit, spending flows toward audit-visible controls regardless of marginal risk reduction, and externalities push private investment below the socially optimal level in exactly the interdependent settings that characterize CI (Gordon et al., 2015). Sociotechnical systems theory explains why the resulting programs underperform: security outcomes emerge from the joint optimization of technical artifacts and social structures, and a regime that optimizes the documentation subsystem while leaving operational practice untouched is a textbook case of partial optimization degrading the whole (Davis et al., 2014; Emery & Trist, 1965; Malatji et al., 2019; Trist & Bamforth, 1951). The observable symptom is the recurring post-incident finding that breached organizations were certified compliant at the moment of compromise, a pattern visible from Ukraine 2015 onward (Lee et al., 2016) and reflected in industry surveys reporting persistent gaps between compliance status and defensive capability (Christopher, 2024; WEF, 2024, 2025).

The dynamic is a familiar one in the theory of measurement: when a proxy becomes a target, it ceases to be a good measure. Audit outcomes are a proxy for security; attaching consequences to the proxy redirects organizational optimization toward the proxy itself. The pathology is subtle because no individual behaves improperly. The compliance manager who prioritizes closing audit findings over hunting for unknown exposures is responding rationally to the incentives the regime creates; the executive who funds the audit-visible control over the higher-value invisible one is doing what governance structures reward; the engineer who documents the intended state rather than the messier actual state is meeting the deadline the evidence calendar imposes. The substitution of compliance for security is thus not a failure of integrity but an emergent property of the incentive architecture, which is precisely why exhortations to treat compliance as a floor rather than a ceiling have had so little effect. Floors attract. As long as the audit is the event on which consequences hang, the audit will be the event around which organizational behavior arranges itself. Two adjacent literatures reinforce the diagnosis. Work on cognitive bias in financial decision-making shows how audit and risk judgments drift toward available, legible evidence and away from harder-to-observe exposures (Fobellah, 2025a), and reviews of the unintended consequences of financial regulation document the same displacement at the level of the firm, where compliance burden absorbs capacity that the regulation was intended to redirect toward the underlying risk (Fobellah, 2025c).

These five failure modes are mutually reinforcing. Static snapshots create the temporal gap; manual limitation ensures the snapshot itself is partial; drift guarantees the environment departs from the snapshot; adversary speed ensures the departure is exploited before the next snapshot; and audit-centric culture ensures organizational energy is directed at the snapshot rather than the gap. The compliance gap in CI is therefore not an implementation failure to be closed by better auditing; it is a design property of periodic assurance itself.

5. THE CASE FOR CONTINUOUS CONTROL

If the diagnosis of Section 4 is correct, the remedy must be architectural rather than procedural: no adjustment of audit frequency, scope, or rigor addresses failure modes that inhere in the episodic form itself. This section assembles the alternative. It proceeds from theoretical foundations (Section 5.1), through the disciplinary lineages that anticipated the shift (Section 5.2), to its codification in standards and regulation (Section 5.3), its architectural expression in zero trust (Section 5.4), and its operational realization in the continuous detection and validation stack (Section 5.5).

5.1 Theoretical Foundations: Control Requires Continuous Feedback

The alternative paradigm has deep theoretical roots. Cybernetics established that regulation of any dynamic system depends on feedback loops whose bandwidth matches the disturbances being regulated (Wiener, 1948); Ashby's (1956) law of requisite variety states the point as a theorem: a controller must command at least as much variety as the environment it controls. A defensive regime that samples its environment annually, against an adversary generating novel states continuously, violates requisite variety by construction. Beer's (1984) viable system model extends the argument to organizations: viability requires real-time operational monitoring channels distinct from, and faster than, periodic managerial review. Read through this lens, the transition from audit to continuous control is not a technology fashion but the restoration of an elementary control-theoretic requirement: the feedback loop must run at the speed of the disturbance.

The cybernetic framing also clarifies what "continuous" must mean in practice, because the term is often diluted to "more frequent." A feedback loop has four components: a sensor, a comparator that evaluates observations against a reference state, an actuator that corrects deviations, and a reference model that is itself kept current. Periodic audit supplies all four, but with a sensing interval of a year, a comparator that runs on human interpretation of documents, an actuator (the corrective action plan) that operates on a timescale of months, and a reference model frozen at the last assessment. Continuous control is not this loop run faster; it is a redesign of each component: telemetry as the sensor, machine-evaluable policy as the comparator, automated or orchestrated response as the actuator, and a living baseline as the reference. The sections that follow trace how each component has matured. Adjacent engineering practice has already completed parts of this redesign. Data-driven digital transformation models for infrastructure delivery treat lifecycle performance as a continuously instrumented property rather than a milestone assessment (Adelanwa et al., 2023), tiered digital twin approaches show how a maintained reference model can support predictive diagnostics even under

resource constraints (Komi & Adeniji, 2023), and digital twin-driven environmental compliance models in oil, gas, and utilities demonstrate the specific move this paper argues for: compliance conclusions derived from a live model of the asset rather than from an assembled evidence package (Ike et al., 2025).

5.2 The Continuous Auditing Heritage

The applied lineage begins, perhaps surprisingly, in accounting. Vasarhelyi and Halper (1991) demonstrated continuous audit of online systems at scale, arguing that when transactions are electronic and continuous, assurance must be too; the subsequent literature developed the architectural patterns (embedded audit modules, monitoring layers, and exception-driven alarms) that modern security telemetry pipelines recapitulate (Alles et al., 2008; Chan & Vasarhelyi, 2011). This literature also documented, importantly, the organizational frictions of the transition: internal audit functions adopted continuous techniques slowly and unevenly, constrained by skills, tooling, and the inertia of cycle-based professional practice (Vasarhelyi et al., 2012), a finding directly prophetic of the difficulties CI operators now face. Contemporary work extends the tradition into cybersecurity oversight proper, surveying AI-assisted continuous auditing systems for technology risk (Aliliele et al., 2025a) and demonstrating continuous audit and threat detection over multi-cloud infrastructure (Torkura et al., 2021). Related work examines what happens when the audited systems are themselves algorithmic, and finds that assurance must then be continuous by necessity, because the object of assurance changes with each retraining (Fobellah, 2025b). Audit analytics in healthcare financial oversight illustrates the same transition in a setting where accountability spans many organizations (Abetoh & Atakpa, 2024), and machine learning applied to fraud detection in banking shows how thoroughly the underlying discipline has already moved from sampling to full-population monitoring (Atakpa & Abetoh, 2022). The intellectual point is settled: assurance frequency is a design variable, and for continuous systems the correct value approaches real time.

A parallel lineage runs through occupational and process safety in other high-hazard industries. Industrial safety assurance was likewise anchored historically in periodic internal audits, that is, QHSE audit systems that verify conformance at scheduled intervals (Obogo et al., 2020), and in retrospective, lagging indicators derived from incident investigation, whose preventive value materializes only after harm has occurred (Obriki & Arumosoye, 2024). The safety field's response anticipated cybersecurity's: systematic exploitation of near-miss and hazard observation data as a continuous signal stream (Arumosoye & Obriki, 2019), proactive hazard identification built on digital safety data streams (Obriki & Arumosoye, 2023), continuous hazard monitoring systems embedded in the workplace (Obriki et al., 2023), and conceptual models linking leading safety signals to sustained injury-free performance (Obriki et al., 2025). Predictive safety analytics extends the pattern further, with models that identify high-risk activity before it is executed (Obogo et al., 2026), applications in liquefied natural gas projects that fold environmental and governance obligations into the same analytic stream (Arumosoye et al., 2026), and data-driven risk control frameworks built specifically for large-scale energy infrastructure (Obriki & Arumosoye, 2018). Automated environmental, social, and governance reporting in energy projects shows the endpoint of the trajectory, where disclosures are generated from operational data rather than compiled for periodic submission (Abioye et al., 2023). That two mature assurance disciplines, financial audit and industrial safety, independently converged on continuous, leading-indicator-driven monitoring strengthens the claim that this shift is a structural requirement of dynamic risk environments rather than a passing fashion of cybersecurity. The convergence is not coincidental. Financial transactions, industrial hazards, and cyber intrusions share a structure: consequential events arise continuously, individually small signals precede them, and the cost of late discovery greatly exceeds the cost of early detection. In each domain, periodic inspection was adopted when observation was expensive and was subordinated once instrumentation made continuous observation cheaper than the losses it prevented. Cybersecurity in critical infrastructure has now crossed the same threshold: the telemetry exists, the storage and analytic capacity exist, and the residual constraint is institutional rather than technical.

5.3 ISCM, CDM, and the Regulatory Turn Toward Continuity

Security standards bodies drew the same conclusion over a decade ago. NIST Special Publication 800-137 defined information security continuous monitoring as maintaining "ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions," explicitly repositioning assessment as a continuous organizational function rather than an event (Dempsey et al., 2011); companion guidance now specifies how to evaluate the ISCM programs themselves (Dempsey et al., 2020). The Risk Management Framework's authorization step was correspondingly reframed toward ongoing authorization, in which the license to operate is continuously earned rather than periodically granted (Joint Task Force, 2018), with control assessment procedures designed for automation (Joint Task Force, 2022). At program scale, the U.S. Continuous Diagnostics and Mitigation program deployed this philosophy across the federal civilian government, standing up continuous asset, identity, and configuration monitoring feeding agency and federal dashboards (CISA, 2020). Executive Order 14028 accelerated the trajectory, mandating endpoint detection and response, log retention, and zero trust migration across federal systems on the explicit premise that periodic assessment had failed (Exec. Order No. 14028, 2021). The NIST CSF itself moved with this current: version 2.0 elevates governance and treats monitoring under the Detect function as an ongoing capability woven through all functions rather than a scheduled activity (NIST, 2024), and CI-focused engineering guidance embeds continuous monitoring into system design rather than bolting it onto operations (Ross et al., 2022). Even the AI systems increasingly used to implement monitoring are themselves brought under a continuous-management lifecycle in the AI Risk Management Framework's map, measure, manage, and govern cycle (NIST, 2023).

Viewed as a sequence, these instruments describe a two-decade regulatory learning curve: from monitoring as a recommended practice (Dempsey et al., 2011), to monitoring as an assessable program (Dempsey et al., 2020), to monitoring as a condition of authorization (Joint Task Force, 2018), to monitoring as a funded federal architecture (CISA, 2020), to monitoring as an executive mandate (Exec. Order No. 14028, 2021). Each step conceded a little more of the premise this paper defends, namely that assurance is a property of a process rather than of an event, and each was driven less by doctrine than by the accumulated experience of certified-but-compromised systems. Sector-specific work has begun to fill in what this means for operators. Cyber risk quantification and governance architectures for critical infrastructure connect continuous posture measurement to executive reporting, closing the loop between telemetry and accountability (Adegbite et al., 2025), and treatments of enterprise network resilience as a national security obligation argue that the object of protection is the continuously available function rather than the certified configuration (Ogunwola & Deborah, 2025). Parallel governance work in digital health, covering artificial intelligence oversight and privacy

compliance (Ekechi et al., 2026) and the data architecture required for interoperability and analytics at national scale (Ilodigwe & Adesemoye, 2021), indicates how far the continuous-governance model has spread beyond the sectors where it originated.

5.4 Zero Trust: Continuous Verification as Architecture

Zero trust architecture generalizes continuous assurance from the organizational level to every individual access decision. Its core tenet, that no trust is implied by network location and that every request is evaluated against dynamic policy using real-time signals about user, device, and context, is continuous control applied at transaction granularity (Rose et al., 2020). Maturity models chart the migration path for agencies and operators (CISA, 2023c), and the academic literature has consolidated the paradigm's mechanisms and evidence base (Buck et al., 2021; Syed et al., 2022). For CI specifically, identity-centric zero trust designs address exactly the drift and lateral-movement failure modes documented above, by making accumulated entitlements and stale trust relationships continuously visible and revocable (Ogbole et al., 2021), and sector studies suggest the model is cost-effective even in resource-constrained critical services such as healthcare (Adebayo et al., 2025). Frameworks developed specifically for operational technology in North American critical infrastructure address the constraints that make naive transplantation unworkable, including legacy protocols, availability requirements, and the safety consequences of enforcement failure (Ahmed et al., 2021). Privacy-centric security engineering makes the complementary architectural argument, embedding the evaluation of access into system design rather than into review cycles (Okoruwa et al., 2020), and regulated healthcare network designs show what continuous verification looks like where statutory confidentiality obligations attach to every transaction (Aliliele et al., 2024b; Ogunwola & Alozie, 2026). Zero trust is thus best understood not as a product category but as the architectural expression of the thesis of this paper: trust, like compliance, decays; both must be re-established continuously.

The connection to the failure modes of Section 4 is direct. Where the static snapshot certifies trust once and assumes it persists, zero trust re-derives trust at every request. Where audit sampling inspects a fraction of access relationships, policy enforcement points mediate all of them. Where drift silently accumulates entitlements, continuous evaluation surfaces and expires them. Zero trust does not eliminate the need for governance, since policies must still be written, identities still proofed, and devices still inventoried, but it relocates verification from the assessment calendar into the request path, which is the only place verification can keep pace with use.

5.5 The Continuous Detection and Validation Stack

A mature continuous control regime rests on three operational layers. The first is continuous observation. Modern detection science supplies the machinery: statistical and machine-learning anomaly detection over network and host telemetry (Buczak & Guven, 2016; Liu & Lang, 2019; Xin et al., 2018), deep learning architectures for intrusion detection at scale (Berman et al., 2019; Ferrag et al., 2020; Shone et al., 2018; Vinayakumar et al., 2019), online ensemble methods capable of learning normal behavior on the wire (Mirsky et al., 2018), and comprehensive treatments of the machine learning role across security operations (Apruzzese et al., 2018, 2023; Dasgupta et al., 2022; Sarker et al., 2020, 2021). AI-augmented engineering research extends these capabilities toward autonomous threat detection and mitigation in software-intensive systems (Odejobi et al., 2025). In the industrial setting specifically, systematic reviews of security information and event management, network detection and response, and anomaly detection architectures for energy sector control networks map what is deployable today against control system constraints (Adegbite et al., 2023). Centralized log analytics and SIEM platforms provide the aggregation substrate that turns distributed telemetry into evaluable compliance and security state (Mbonu et al., 2019b), and security analytics increasingly integrates forensic depth for after-the-fact reconstruction (Ogbole et al., 2025).

The second layer is continuous response. Detection without timely action merely timestamps failure; security orchestration, automation, and response frameworks close the loop by encoding containment playbooks that execute at machine speed under human governance (Dosunmu & Ogundele, 2025c; Islam et al., 2019). Organizationally, this drives the integration of network and security operations centers into unified, continuously staffed functions (Ladapo et al., 2024a; Vielberth et al., 2020).

The third layer, and the most direct successor to the audit, is continuous validation of the controls themselves. Rather than asking annually whether controls are documented, breach-and-attack simulation and adversary emulation frameworks exercise controls perpetually against catalogued adversary techniques, measuring whether the defensive stack actually prevents, detects, and responds as claimed (Dosunmu & Ogundele, 2024a, 2025a). Threat-informed defense engineering formalizes the measurement of control effectiveness at scale (Dosunmu & Ogundele, 2024d), and enterprise models for continuous security validation in regulated infrastructures show how such evidence can feed compliance reporting directly, collapsing the distinction between security operations and audit evidence (Dosunmu & Ogundele, 2024c). Quantification frameworks translate the resulting effectiveness data into risk-based investment prioritization (Dosunmu & Ogundele, 2024b), and performance measurement frameworks deliver it to boards and regulators in decision-ready form (Dosunmu & Ogundele, 2025b), restoring, on a continuous basis, the governance visibility that was the periodic audit's principal legitimate function. The forecasting methods this layer depends on are mature in adjacent domains: demand forecasting with machine learning for financial planning (Tonoyan et al., 2021), interpretable failure prediction for distributed energy assets (Komi & Adamolekun, 2021), real-time risk dashboards in hospital supply chains (Filani et al., 2022), predictive analytics embedded in resilient logistics systems (Anene & Clement, 2022), and predictive power management for intermittent devices operating under uncertain energy availability (Asiedu et al., 2026) all demonstrate that continuously updated projections can be made accurate enough to act on, which is the technical premise of continuous assurance. The market has followed the logic: continuous threat exposure management now features among leading strategic technology trends precisely because point-in-time assessment is recognized as inadequate (Gartner, 2023).

The three layers are complementary rather than redundant, and the regime degrades predictably when any one is absent. Observation without validation sees events but cannot say whether controls would withstand an attack that has not yet occurred; validation without observation proves that controls worked at the moment of the test but not that they are working now; and either without response merely produces better-documented failures. Together, however, they invert the audit's epistemology: instead of inferring operational reality from curated artifacts, the organization derives its compliance artifacts from operational reality. Evidence is no longer produced for the assessor; it is a byproduct of defense.

Regulatory practice is beginning to align with this stack. The NERC CIP internal network security monitoring requirement will make continuous east-west observation a compliance obligation for high-impact and externally connected medium-impact systems in the electric sector, phased in

over the period to 2030 (CIP-015-1, 2025); cross-sector performance goals emphasize detection and response capabilities rather than documentation (CISA, 2023b); and the U.K. Cyber Assessment Framework assesses outcomes, including security monitoring, as standing capabilities (NCSC, 2024). The direction of travel is unmistakable, even where the pace lags the threat environment: the object of assurance is shifting from the document to the telemetry.

6. DISCUSSION AND IMPLICATIONS

6.1 Continuous Control Is Necessary but Not Sufficient

The case assembled above should not be read as technological triumphalism. Continuous monitoring inherits hard, well-documented problems. The base-rate fallacy guarantees that even highly accurate detectors produce overwhelming false-positive volumes when true intrusions are rare (Axelsson, 2000), and machine learning approaches to intrusion detection face structural difficulties (concept drift, semantic gaps between anomalies and attacks, and evaluation pathologies) that two decades of research have catalogued rather than solved (Arp et al., 2022; Sommer & Paxson, 2010). Operationally, alert overload is the defining pathology of security operations centers: analysts report false-positive rates that make triage Sisyphean (Alahmadi et al., 2022), burnout is endemic (Sundaramurthy et al., 2015), and organizational misalignments between SOC mandates and resources are common (Kokulu et al., 2019). Automated triage and contextual analysis mitigate but do not eliminate the problem (Hassan et al., 2019; van Ede et al., 2022). Automation itself introduces new failure modes: complacency and automation bias degrade human oversight exactly where it is most needed (Goddard et al., 2012; Parasuraman & Manzey, 2010), continuous AI-driven defense creates a new attack surface for adversarial manipulation (Biggio & Roli, 2018), and delegating security judgment to opaque models is a double-edged sword requiring deliberate governance (Taddeo et al., 2019). Adversarial machine learning framed specifically for critical infrastructure shows how the risk changes when the manipulated model governs a physical process (Adebayo et al., 2022), and reviews of artificial intelligence's role in modern cybersecurity are candid that capability gains and new dependencies arrive together (Hussain & Adebayo, 2026). Comparable assessments in clinical settings, where automated decision support is deployed under strict accountability requirements, reach the same balance of promise and implementation risk (Ilodigwe & Adesemoye, 2025a). Human-in-the-loop designs that keep expert judgment inside automated pipelines are therefore a design requirement, not an optional refinement (Ladapo et al., 2022a). The design problem is harder than it appears: human-centered annotation work shows how much the quality of automated output depends on the structure of the human contribution (Ladapo et al., 2024b), and studies of the disagreement problem in human-in-the-loop federated learning show that expert judgment is itself variable and must be treated as a modeled input rather than an authoritative oracle (Ladapo et al., 2026). Telemetry is not free at the edge either. Analyses of the energy, reliability, and latency trade-offs governing green communication for next-generation IoT show that observation, transmission, and responsiveness compete for one constrained budget (Asiedu & Quainoo, 2024), and conceptual work characterizing those trade-offs makes clear that continuous monitoring of resource-limited devices is an engineering optimization rather than a matter of switching telemetry on (Asiedu et al., 2025).

For OT environments the constraints are sharper still. Passive monitoring must be engineered so that observation cannot perturb safety-critical processes; legacy protocols lack the instrumentation continuous control presumes; and the interaction between safety and security demands co-engineering rather than IT-pattern transplantation (Kriaa et al., 2015; Stouffer et al., 2023). Continuous control in CI will therefore mature unevenly, sector by sector, and hybrid regimes, meaning continuous telemetry within a periodic governance envelope, are the realistic medium-term destination.

Honesty about these limits also disciplines the transition's sequencing. An operator who cannot yet maintain an accurate asset inventory will not benefit from adversary emulation; a security operations center drowning in unactioned alerts gains nothing from additional telemetry sources. The continuous control stack is a dependency graph, not a shopping list: asset visibility precedes meaningful monitoring, monitoring precedes meaningful response automation, and response maturity precedes the safe use of continuous validation, which deliberately generates attack-like activity that an unprepared operations function will either ignore or misclassify. Programs that skip layers convert continuous control from an assurance architecture into a more expensive form of shelfware, and hand skeptics of the paradigm an easy refutation. The limits discussed in this subsection are limits of the proposed remedy; the limitations of the present study, including the composition of its evidence base and the inferences it can support, are stated separately in Section 7.

6.2 Implications for Regulators, Operators, and Auditors

For regulators, the implication is a shift in the object of supervision: from certifying documents to certifying capabilities, and ultimately to consuming operator telemetry. Instruments already exist on this continuum, including continuous diagnostics dashboards (CISA, 2020), outcome-based assessment frameworks (NCSC, 2024), and mandatory internal monitoring (CIP-015-1, 2025), but harmonization across regimes such as NIS2, NERC CIP, and CSF-based oversight remains undone (NIS 2 Directive, 2022; ENISA, 2025). Regulators must also resist reproducing the audit-centric pathology in continuous form: if operators are graded on dashboard color rather than validated control effectiveness, gaming will simply accelerate (Jaquith, 2007).

For operators, the transition is as much organizational as technical. Sociotechnical systems theory predicts, and the continuous auditing adoption literature confirms, that grafting continuous tooling onto cycle-based governance structures yields disappointment (Malatji et al., 2019; Vasarhelyi et al., 2012). Roles must change: compliance teams become consumers of live control-effectiveness data; audit preparation dissolves into everyday hygiene; and scarce expertise is redirected from evidence assembly to detection engineering and validation design (Dosunmu & Ogundele, 2024c; Furnell, 2017). Change management research supplies the template. Strategic frameworks for building resilient organizations emphasize that capability, not technology acquisition, is the binding constraint (Ilodigwe & Adesemoye, 2024); large-scale transformation models show that the sequencing and governance of change determine whether new capability is absorbed or abandoned (Ilodigwe & Adesemoye, 2025b); and work on standard operating procedures as strategic assets identifies the mundane mechanism through which new practice becomes durable (Eyetsemitan et al., 2022). Project governance research in multinational infrastructure environments (Amayo et al., 2023) and lifecycle management practice for data center programs, where security, efficiency, and compliance obligations must be reconciled continuously (Amayo et al., 2024), both describe the coordination structures such transitions require. Investment logic changes correspondingly: continuous effectiveness data finally supplies the

feedback that economic models of security investment have always lacked, allowing spending to track measured marginal risk reduction rather than audit visibility (Gordon & Loeb, 2002; Gordon et al., 2020). Quantitative risk allocation architectures developed for public-private partnerships offer a model for distributing such measurements across parties with different obligations (Ike et al., 2024), and predictive vendor risk assessment applies the same logic to the supplier estate, where exposure is continuous while procurement decisions are periodic (Tonoyan et al., 2024a).

For the audit profession, the lesson of the accounting literature applies directly: continuous techniques did not eliminate auditors, but they did transform the auditor's role from evidence sampler to designer and verifier of monitoring systems (Alles et al., 2008; Chan & Vasarhelyi, 2011). The cybersecurity assessor's future analog is the validation architect, the professional who designs the adversary emulations, verifies the telemetry pipelines, and attests that the continuous control system itself is trustworthy (Dosunmu & Ogundele, 2025a; Joint Task Force, 2022).

Sequencing also matters at the regime level. A plausible transition path runs in three stages. First, regulators accept continuously generated evidence in satisfaction of existing periodic requirements: the operator's telemetry and validation records replace the manually assembled evidence package, reducing cost without changing the compliance framework. Second, requirements themselves are restated as continuously verifiable properties: not "access reviews shall be performed quarterly" but "no account shall retain entitlements unused for ninety days," a formulation a machine can check every day rather than an assessor on one. Third, supervision becomes exception-based: regulators define the telemetry and effectiveness thresholds that constitute good standing, and assessment effort concentrates on operators whose signals degrade. Each stage preserves the audit's accountability function while progressively replacing its epistemology, and each is already visible in embryonic form in the instruments surveyed above.

6.3 Research Agenda

Three research gaps merit emphasis. First, measurement: the field lacks validated metrics linking continuous monitoring coverage to realized risk reduction in CI settings, extending resilience metric foundations into the compliance domain (Linkov et al., 2013; Pfleeger & Cunningham, 2010). Second, OT-specific detection science: the anomaly detection literature remains overwhelmingly IT-centric, while cyber-physical processes offer physics-based invariants that detection research has only begun to exploit (Ahmed et al., 2016; Cárdenas et al., 2011; Humayed et al., 2017). Third, the political economy of continuous supervision: telemetry-based regulation raises unresolved questions of liability, confidentiality, and regulator capacity that legal and governance scholarship has yet to address systematically (Gordon et al., 2015; WEF, 2025). A fourth, more practical gap cuts across the other three: transition economics. The literature documents why continuous control is necessary and how its components work, but it offers CI operators little guidance on staging investments under real constraints such as regulated rate recovery, decade-long procurement cycles, and workforces sized for compliance rather than engineering. Comparative case studies of operators at different transition stages would do more to accelerate adoption than further demonstrations of technical feasibility. Infrastructure research outside cybersecurity suggests where to look for method. Performance metric frameworks for long-lived healthcare assets address the same problem of linking sustained investment to measurable outcomes (Aminu-Ibrahim et al., 2025b); econometric work on just transition in energy systems shows how distributional consequences can be quantified rather than asserted (Komi & Adamolekun, 2024); and modeling of the causal link between community trust and infrastructure durability demonstrates that institutional variables often thought too soft to measure can in fact be operationalized (Komi & Adeniji, 2024). Assurance research would benefit from the same insistence on measurement.

7. LIMITATIONS

The argument above is a conceptual synthesis, and its limitations are those of that genre rather than those of an underpowered experiment. They are stated here in full because several of them bear directly on how much weight the paper's central claim can carry.

Review design. This is a narrative conceptual review, not a systematic one. Sources were selected for argumentative relevance rather than through a pre-registered protocol with named databases, disclosed search strings, explicit inclusion and exclusion criteria, dual screening, and formal quality appraisal. The synthesis is therefore exposed to selection and confirmation bias in a specific and asymmetric way: literature supporting a discontinuity between certification and security was sought actively, while literature reporting that periodic assessment performs adequately in particular settings was not hunted for with equal energy. The five failure modes should accordingly be read as an analytic framework offered for testing, not as a validated taxonomy, and the absence of contrary evidence in these pages is weak evidence of its absence in the field.

Composition of the evidence base. The reference base is concentrated rather than broad. A substantial share of the cited work comes from a connected cluster of recent journals and author groups working on operational technology assurance, continuous validation, and adjacent governance topics, identified in Section 1.1. Much of that work is conceptual or review-based rather than experimental, and several of the venues involved do not carry the peer-review track record of the established security and accounting literature also cited here. Where a proposition rests only on that cluster it should be read as convergent framing rather than as independent corroboration. The load-bearing empirical anchors of the argument, namely the incident analyses, the detection-science findings on base rates and alert volume, the standards and regulatory instruments, and the continuous auditing literature, are drawn from established sources and can be assessed on their own terms.

Case selection and inference. Section 2.3 relies on three heavily documented incidents, chosen precisely because they are unusually well described in the public record. That is a selection criterion, not a sampling frame. Intrusions detected early, contained quietly, or never disclosed are absent by construction, and their absence biases the account toward the conclusion that detection fails. Public technical reporting on these cases is also asymmetric: it establishes attacker tradecraft in considerable detail while saying almost nothing about the victims' internal assurance arrangements. Inferences about what a compliance apparatus did or did not register in these organizations are therefore illustrative rather than evidentiary, and Section 2.3 has been written to say so.

Absence of an effect estimate. The paper argues that continuous control is a better-matched assurance architecture for the environment described in Section 2. It does not demonstrate that adopting it reduces realized risk. No study cited here establishes that operators running continuous monitoring programs experience fewer or less severe compromises than comparable operators relying on periodic assessment, holding sector, maturity, and threat exposure constant, and the counterfactual is not recoverable from the public record. The central claim is a design argument,

not an effect size. The cost side is likewise unaddressed: continuous control carries capital, staffing, and operational-risk costs, including the risk that active validation perturbs a live process, and a complete appraisal would weigh those against the cost of the periodic regime it replaces. No such appraisal is attempted here, which is one reason the research agenda in Section 6.3 gives transition economics a prominent place.

Regulatory currency and jurisdictional scope. The regulatory analysis is a snapshot of instruments that are actively moving, and it draws almost entirely on the United States, the European Union, and the United Kingdom. Regimes in other jurisdictions are not represented, and no claim of global generalizability is made. Two distinctions deserve emphasis for readers checking the argument later: an instrument that has been approved may not yet be in force, and one that is in force may not yet bind operators, because phased implementation can defer practical effect by years. CIP-015-1 illustrates both. Statements here about what regulation currently requires should be verified against each instrument's own effective and implementation dates at the time of reading.

Sectoral generalization. Critical infrastructure is treated throughout as a single analytic category, and it is not one. The sectors differ in ways the argument does not fully accommodate. Electricity has mandatory audited standards and comparatively mature operational telemetry, and it supplies most of the paper's regulatory evidence. Water and wastewater is dominated by small utilities with no dedicated security staff, for which the three-layer stack described in Section 5.5 is not currently affordable at any sequencing. Healthcare's binding constraint is device certification rather than network architecture. Conclusions drawn from the electric sector should not be transferred to the others without adjustment, and the uneven, sector-by-sector maturation anticipated in Section 6.1 is a consequence of this heterogeneity rather than a concession to it.

8. CONCLUSION

This paper has argued that the periodic, audit-based compliance model that still dominates critical infrastructure cybersecurity is structurally, not incidentally, incapable of ensuring real-time security. Five failure modes compound one another: audits measure the past while attackers operate in the present; manual assessment samples a shrinking fraction of an expanding estate; configuration drift dissolves the certified state within days of certification; adversary operational tempo outpaces assurance cycles by orders of magnitude; and audit-centric incentives redirect organizational energy from risk reduction to evidence production. In an environment defined by IT/OT convergence, industrial IoT proliferation, systemic interdependency, pre-positioned nation-state access, and industrialized ransomware, the resulting compliance gap is a national-security liability, not a paperwork problem.

The argument's structure bears restating, because its force is cumulative rather than local. Any one failure mode, taken alone, could be treated as an implementation defect and met with an incremental remedy: audit more often, sample more widely, document more carefully. It is the interaction of the five that forecloses this response. More frequent audits do not help when each audit still measures curated artifacts rather than live state; wider sampling does not help when the population grows faster than the sample; better documentation does not help when the incentive structure rewards the documentation itself. The periodic model fails not at its edges but at its center, at the assumption, inherited from a slower technological era, that an environment inspected occasionally remains approximately the environment that was inspected. Critical infrastructure has not satisfied that assumption for years.

The remedy has a coherent lineage and an accumulating regulatory mandate: continuous auditing theory from accounting information systems, information security continuous monitoring and continuous diagnostics from the standards community, zero trust as continuous verification at transaction granularity, and continuous control validation as the operational successor to the audit. The transition is demanding, and the obstacles are genuine: alert overload, automation bias, adversarial pressure on defensive AI, and OT safety constraints. These are nonetheless engineering and governance problems within the correct paradigm, whereas the failure modes of periodic compliance are defects of the paradigm itself. For critical infrastructure, the question is no longer whether assurance must become continuous, but how quickly regulators, operators, and the assurance profession can rebuild their institutions around a simple control-theoretic truth: a defense that is verified occasionally is, from the adversary's point of view, a defense that is unverified almost always.

None of this will happen quickly, and the intermediate state carries its own obligations. For years to come, most CI operators will live in hybrid regimes: continuous telemetry feeding periodic governance, machine-generated evidence attached to human-scheduled attestations. Managed deliberately, the hybrid is a bridge, with each assessment cycle absorbing more continuously generated evidence until the assessment becomes a review of the monitoring system rather than of the environment it monitors. Managed complacently, the hybrid is a resting place in which dashboards decorate an unchanged audit culture. The difference between the two outcomes is not technological; it is a matter of whether regulators, boards, and the assurance profession internalize the conclusion this review has assembled: in critical infrastructure, security is a property of the present tense, and an assurance regime that cannot speak in the present tense cannot, in any meaningful sense, assure.

DECLARATIONS

Ethics approval and consent to participate. Not applicable. This study is a conceptual review of published literature, standards documents, regulatory instruments, and publicly available incident and industry reports. It involved no human participants, no animal subjects, and no personal or identifiable data, and therefore required neither institutional review board approval nor informed consent.

Consent for publication. Not applicable. The manuscript contains no individual person's data in any form.

Availability of data and materials. No new data were generated or analysed. All sources on which the argument rests are listed in the reference list; the standards, regulatory instruments, government publications, and industry reports are publicly accessible at the locations cited, and the scholarly sources are available from their respective publishers.

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. No organization had any role in the design of the study, in the selection or interpretation of sources, in the writing of the manuscript, or in the decision to submit it for publication.

Competing interests. The author declares no financial or non-financial competing interests. The author holds no consulting relationship, advisory role, equity position, or paid engagement with any vendor of continuous monitoring, security validation, or compliance software, nor with any

regulator, standards development organization, or assurance provider discussed in this paper. Commercial publications from named vendors and market research firms are cited as industry telemetry, are identified as such in Section 2.3, and are subject to the self-selection and methodological-opacity caveats stated in Section 7. Their citation does not constitute endorsement of the products or services of the organizations concerned.

Prior publication and overlap with related work. This manuscript is original, has not been published previously in whole or in part, and is not under consideration by any other venue. Its relationship to closely related earlier work in the same research area, including what that work established and what is claimed as new here, is set out in Section 1.1. No text, figure, table, or result from any prior publication is reproduced in this manuscript.

Author contributions. The single author is responsible for conceptualization, methodology, literature identification and synthesis, analysis, drafting of the original manuscript, and revision, and approves the submitted version.

Use of AI-assisted technologies. Generative AI tools were used solely for language editing and reference formatting. No AI system was used to generate, select, or interpret source material, to produce the analysis, or to draw the conclusions presented. The author reviewed all output, takes full responsibility for the content and integrity of the work, and confirms that no AI system is listed or credited as an author.

REFERENCES

1) Abetoh, N. F., & Atakpa, M. I. (2024). Audit analytics in healthcare financial oversight: Leveraging data science to strengthen accountability in multilateral grant ecosystems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(6), 2710–2747. https://doi.org/10.32628/CSEIT2410791
2) Abioye, R. F., Okojie, J. S., Filani, O. M., Ike, P. N., Idu, J. O. O., Nnabueze, S. B., Okojokwu-Idu, J. O., & Ihwughwavwe, S. I. (2023). Automated ESG reporting in energy projects using blockchain-driven smart compliance management systems. *International Journal of Multidisciplinary Evolutionary Research*, *4*(2), 120–129. https://doi.org/10.54660/IJMER.2023.4.2.120-129
3) Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2022). Adversarial machine learning in critical infrastructure: A conceptual framework for threat modeling AI enabled OT systems. *World Journal of Innovation and Modern Technology*, *6*(1), 184–234. https://doi.org/10.56201/wjimt.v6.no1.2022.pg184.234
4) Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2023). AI augmented threat detection in industrial control systems: A systematic review of machine learning approaches for ICS anomaly detection. *International Journal of Engineering and Modern Technology*, *9*(3), 287–340. https://doi.org/10.56201/ijcsmt.v9.no3.2023.pg287.340
5) Adebayo, A., Anunagba, C. O., & Ozowara, D. E. (2025). A review of zero trust security models and cost effectiveness in healthcare infrastructure. *International Journal of Advanced Multidisciplinary Research and Studies*, *5*(6), 2269–2283. https://doi.org/10.62225/2583049X.2025.5.6.6051
6) Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2020). Securing operational technology networks in electric utilities: A systematic review of NERC CIP compliance and architectural threat mitigation. *International Journal of Engineering and Modern Technology*, *6*(3), 103–146. https://doi.org/10.56201/ijemt.vol.6.no3.2020.pg103.146
7) Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2022). A security architecture model for IT and OT convergence in regulated energy networks: Design principles and governance alignment. *International Journal of Computer Science and Mathematical Theory*, *8*(2), 81–132. https://doi.org/10.56201/ijcsmt.v8.no2.2022.pg81.132
8) Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2023). ICS and SCADA threat detection architectures in energy sector networks: A systematic review of SIEM, NDR, and anomaly detection approaches. *World Journal of Innovation and Modern Technology*, *7*(2), 121–182. https://doi.org/10.56201/wjimt.v7.no2.2023.pg121.182
9) Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024a). A vulnerability governance architecture for power and utilities corporations: From exposure mapping to remediation verification. *World Journal of Innovation and Modern Technology*, *8*(6), 185–246. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.246
10) Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024b). An AI driven security operations architecture for utility sector SOCs: Integrating threat intelligence, behavioral analytics, and automated response. *International Journal of Engineering and Modern Technology*, *10*(11), 197–256. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.256
11) Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2025). A cyber risk quantification and governance architecture for critical infrastructure: From posture measurement to executive reporting. *International Journal of Computer Science and Mathematical Theory*, *11*(12), 232–293. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg232.293
12) Adelanwa, A., Basnet, A., & Anene, U. N. (2023). Data driven digital transformation models for lifecycle performance management in infrastructure delivery. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2646–2662. https://doi.org/10.62225/2583049X.2023.3.6.5968
13) Adenuga, O. M. (2022). Smart grid architectures and energy distribution for high renewable penetration: A comprehensive review of technologies, operations, and deployment pathways. *International Journal of Engineering and Modern Technology*, *8*(5), 125–155. https://doi.org/10.56201/ijemt.v8.no5.2022.pg125.155
14) Adeyelu, O. O. (2018). A predictive compliance monitoring framework for detecting systemic safety risks through aviation consumer complaint data. *Iconic Research and Engineering Journals*, *1*(8), 250–276. https://doi.org/10.64388/IREV1I8-1718478
15) Adeyelu, O. O. (2019). An adaptive safety management system implementation model for aerodromes in developing economy contexts. *Iconic Research and Engineering Journals*, *3*(4), 628–654. https://doi.org/10.64388/IREV3I4-1718479
16) Adeyelu, O. O., & Dagodzo, D. (2022). A comparative benchmarking model for aerodrome certification compliance across developing economy civil aviation authorities. *International Journal of Multidisciplinary Research and Growth Evaluation*, *3*(6), 1016–1035. https://doi.org/10.54660/.IJMRGE.2022.3.6.1016-1035

17) Adeyelu, O. O., & Dagodzo, D. (2024). A maturity model for predicting airport safety audit outcomes in resource-constrained regulatory environments. *International Journal of Scientific Research in Civil Engineering*, *8*(4), 132–170. https://doi.org/10.32628/IJSRCE248423
18) Agbabiaka, J., Okonkwo, C. S., Ogunwole, O., Mayo, W., & Okeke, O. T. (2019). Supply chain risk management model for EPC and gas processing projects. *Iconic Research and Engineering Journals*, *3*(2), 968–980. https://doi.org/10.64388/IREV3I2-1713124
19) Agu, M. U., Akomolafe, O., & Bello, A. (2023). A comparative review of SOX compliance frameworks in cross-border financial auditing. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2297–2306. https://doi.org/10.62225/2583049X.2023.3.6.5362
20) Ahmed, M. O., Adegbite, M. P., & Adebayo, A. (2021). Zero trust architecture for operational technology in North American critical infrastructure: A framework for implementation and resilience optimization. *International Journal of Engineering and Modern Technology*, *7*(1), 66–113. https://doi.org/10.56201/ijemt.vol.7.no1.2021.pg66.113
21) Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
22) Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. *Iconic Research and Engineering Journals*, *1*(9), 476–492. https://doi.org/10.64388/IREV1I9-1713778
23) Akin-Oluyomi, O. T., Atima, M. E., & Akinleye, O. K. (2023). Regulatory compliance and supplier risk assessment frameworks in international pharmaceutical procurement. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2194–2204.
24) Akinleye, O. K., & Adeyoyin, O. (2021). Process automation framework for enhancing procurement efficiency and transparency. *Shodhshauryam, International Scientific Refereed Research Journal*, *4*(4), 356–387.
25) Akomolafe, O., & Agu, M. U. (2018). A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. *Iconic Research and Engineering Journals*, *1*(9), 458–475.
26) Akomolafe, O., Agu, M. U., & Bello, A. (2023). A conceptual model for implementing risk-based auditing in strategic financial management. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2274–2286. https://doi.org/10.62225/2583049X.2023.3.6.5359
27) Akomolafe, O., Agu, M. U., & Bello, A. (2025). A conceptual model for advancing risk governance through data-driven compliance analytics in financial institutions. *Journal of Accounting and Financial Management*, *11*(11), 211–228. https://doi.org/10.56201/jafm.vol.11.no11.2025.pg211.228
28) Alahmadi, B. A., Axon, L., & Martinovic, I. (2022). 99% false positives: A qualitative study of SOC analysts' perspectives on security alarms. In *Proceedings of the 31st USENIX Security Symposium* (pp. 2783–2800). USENIX Association. https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi
29) Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002
30) Alexander, O., Belisle, M., & Steele, J. (2020). *MITRE ATT&CK for industrial control systems: Design and philosophy*. The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf
31) AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054
32) Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2023). A conceptual framework for continuous cloud misconfiguration monitoring and enterprise risk mitigation strategies. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *9*(10), 373–394. https://doi.org/10.32628/CSEIT2361071
33) Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024a). A conceptual framework for enterprise data sensitivity classification and regulatory traceability mechanisms. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 3103–3124. https://doi.org/10.62225/2583049X.2024.4.6.5991
34) Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024b). Advances in HIPAA compliant data architecture and secure analytics frameworks for community healthcare organizations. *Shodhshauryam, International Scientific Refereed Research Journal*, *7*(2), 277–324. https://doi.org/10.32628/SHISRRJ2472163
35) Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025a). A review of AI assisted continuous auditing systems in technology risk and cybersecurity oversight. *Gyanshauryam, International Scientific Refereed Research Journal*, *8*(4), 210–250. https://doi.org/10.32628/GISRRJ258369
36) Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025b). Advances in data lakehouse governance architectures for enterprise data loss prevention and compliance assurance. *Shodhshauryam, International Scientific Refereed Research Journal*, *8*(4), 171–213. https://doi.org/10.32628/SHISRRJ258474
37) Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems*, *22*(2), 195–214. https://doi.org/10.2308/jis.2008.22.2.195
38) Amayo, E. B., Owulade, O. A., & Isi, L. R. (2023). Optimizing project governance in multinational infrastructure projects: Insights from General Electric's global operations. *International Journal of Multidisciplinary Research and Growth Evaluation*, *4*(1), 975–983. https://doi.org/10.54660/.IJMRGE.2023.4.1.975-983
39) Amayo, E. B., Owulade, O. A., & Isi, L. R. (2024). Best practices for managing data center lifecycle projects: Ensuring security, efficiency, and compliance in U.S. enterprises. *Iconic Research and Engineering Journals*, *7*(7), 598–617.
40) Aminu-Ibrahim, A. Y., Ogbete, J. C., & Ambali, K. B. (2024). Governance and accountability models for public private partnerships in healthcare infrastructure development. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 2943–2960.

Corresponding Author: Chukwunenye Amadi

https://doi.org/10.62225/2583049X.2024.4.6.5699

41) Aminu-Ibrahim, A. Y., Ogbete, J. C., & Iwuanyanwu, O. C. (2025a). Infrastructure resilience planning for national diagnostic systems under public health stress conditions. *Gyanshauryam, International Scientific Refereed Research Journal*, *8*(1), 340–381. https://doi.org/10.32628/GISRRJ2582311
42) Aminu-Ibrahim, A. Y., Ogbete, J. C., & Iwuanyanwu, O. C. (2025b). Sustainable healthcare infrastructure performance metrics for long-term asset management and value creation. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(4), 566–601. https://doi.org/10.32628/CSEIT251116277
43) Anene, U. N., & Clement, T. (2022). A resilient logistics framework for humanitarian supply chains: Integrating predictive analytics, IoT, and localized distribution to strengthen emergency response systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *8*(5), 398–424.
44) Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211
45) Annan, A. O. (2025). Cybersecurity compliance as a source of competitive advantage in technology markets. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(5), 456–487.
46) Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 371–390). NATO CCD COE. https://doi.org/10.23919/CYCON.2018.8405026
47) Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. *Digital Threats: Research and Practice*, *4*(1), 1–38. https://doi.org/10.1145/3545574
48) Arp, D., Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., & Rieck, K. (2022). Dos and don'ts of machine learning in computer security. In *Proceedings of the 31st USENIX Security Symposium* (pp. 3971–3988). USENIX Association. https://www.usenix.org/conference/usenixsecurity22/presentation/arp
49) Arumosoye, O. M., & Obriki, O. D. (2019). Systematic review of near-miss and hazard observation data utilization in industrial safety management. *Iconic Research and Engineering Journals*, *3*(2), 981–999. https://doi.org/10.64388/IREV3I2-1714417
50) Arumosoye, O. M., Obriki, O. D., & Ozobu, C. O. (2026). Systematic review of predictive safety analytics applications in LNG projects with ESG implications. *Global Journal of Engineering and Technology Review*, *2*(2), 61–73. https://doi.org/10.65150/EP-gjetr/V2E2/2026-05
51) Ashby, W. R. (1956). *An introduction to cybernetics*. Chapman & Hall.
52) Asiedu, W., & Quainoo, R. (2023a). How far can energy harvesting take us? A systematic review of radio frequency strategies for energy autonomous sensing. *Shodhshauryam, International Scientific Refereed Research Journal*, *6*(1), 448–466.
53) Asiedu, W., & Quainoo, R. (2023b). Toward maintenance free wireless infrastructure: Simulating performance and reliability in large scale intermittently powered IoT networks. *Gyanshauryam, International Scientific Refereed Research Journal*, *6*(1), 489–510.
54) Asiedu, W., & Quainoo, R. (2024). Rethinking energy, reliability, and latency trade-offs in green communication for next generation IoT. *International Journal of Multidisciplinary Research and Growth Evaluation*, *5*(6), 1987–1994.
55) Asiedu, W., & Quainoo, R. (2025). GleanCast: Epoch-aligned reliable broadcast in batteryless intermittent sensor networks. *International Journal of Engineering and Modern Technology*, *11*(12), 205–218. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg205.218
56) Asiedu, W., Quainoo, R., & Asiedu, A. (2025). A conceptual framework for characterizing fundamental energy, reliability, and latency trade-offs in green communication paradigms for next-generation IoT. *International Journal of Advanced Multidisciplinary Research and Studies*, *5*(6), 2447–2453. https://doi.org/10.62225/2583049X.2025.5.6.6479
57) Asiedu, W., Quainoo, R., & Asiedu, A. (2026). Predictive power management for intermittent IoT devices using lightweight machine learning under uncertain energy harvest. *Gulf Journal of Engineering and Technology*, *2*(4), 108–118.
58) Atakpa, M. I., & Abetoh, N. F. (2022). A systematic review of machine learning advances in financial fraud detection for banking systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *8*(2), 771–801. https://doi.org/10.32628/CSEIT23906220
59) Atakpa, M. I., & Fobellah, A. N. (2023). Anomaly detection in financial time-series data: A conceptual model for healthcare and banking applications. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *9*(2), 967–997. https://doi.org/10.32628/CSEIT2342441
60) Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security*, *3*(3), 186–205. https://doi.org/10.1145/357830.357849
61) Beer, S. (1984). The viable system model: Its provenance, development, methodology and pathology. *Journal of the Operational Research Society*, *35*(1), 7–25. https://doi.org/10.1057/jors.1984.2
62) Bello, A. D., Elebe, O., Hammed, N. I., Omoegun, G. O., & Fadayomi, O. (2024). A cybersecurity risk management and regulatory compliance framework for financial institutions. *Iconic Research and Engineering Journals*. https://www.irejournals.com/paper-details/1713553
63) Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, *10*(4), Article 122. https://doi.org/10.3390/info10040122
64) Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys & Tutorials*, *16*(1), 303–336. https://doi.org/10.1109/SURV.2013.052213.00046
65) Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, *84*, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

66) Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015
67) Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*(102436), Article 102436. https://doi.org/10.1016/j.cose.2021.102436
68) Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
69) Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690
70) Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems*, *12*(2), 152–160. https://doi.org/10.1016/j.accinf.2011.01.001
71) Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), Article 15. https://doi.org/10.1145/1541880.1541882
72) Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009
73) Christopher, J. D. (2024). *SANS 2024 state of ICS/OT cybersecurity [Survey report]*. SANS Institute. https://www.sans.edu/cyber-research/sans-2024-state-ics-ot-cybersecurity
74) Claroty. (2024). *The global state of CPS security 2024: Business impact of disruptions*. Claroty Ltd. https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions
75) Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.
76) Critical Infrastructure Protection Reliability Standard CIP-015-1: Cyber security, internal network security monitoring, 90 Fed. Reg. (July 2, 2025). https://www.federalregister.gov/documents/2025/07/02/2025-12309/critical-infrastructure-protection-reliability-standard-cip-015-1-cyber-security-internal-network
77) Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202
78) Cybersecurity and Infrastructure Security Agency. (2020). *Continuous Diagnostics and Mitigation (CDM) program overview [Fact sheet]*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_CDM%20Program%20Overview_Fact%20Sheet_1.pdf
79) Cybersecurity and Infrastructure Security Agency. (2023a). *People's Republic of China state-sponsored cyber actor living off the land to evade detection*. Joint Cybersecurity Advisory AA23-144A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
80) Cybersecurity and Infrastructure Security Agency. (2023b). *Cross-sector cybersecurity performance goals (March 2023 update)*. U.S. Department of Homeland Security. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
81) Cybersecurity and Infrastructure Security Agency. (2023c). *Zero trust maturity model, Version 2.0*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
82) Cybersecurity and Infrastructure Security Agency. (2024). *PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure*. Joint Cybersecurity Advisory AA24-038A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
83) Cybersecurity and Infrastructure Security Agency. (n.d.a). *Reducing the significant risk of known exploited vulnerabilities [Known Exploited Vulnerabilities Catalog]*. U.S. Department of Homeland Security. https://www.cisa.gov/known-exploited-vulnerabilities
84) Cybersecurity and Infrastructure Security Agency. (n.d.b). *Shields Up: Guidance for organizations*. U.S. Department of Homeland Security. https://www.cisa.gov/shields-up
85) Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., & Sastry, S. (2011). Attacks against process control systems: Risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 355–366). ACM. https://doi.org/10.1145/1966913.1966959
86) Dagodzo, D. (2018). A conceptual framework for UAV integration into national power grid inspection programs. *Iconic Research and Engineering Journals*, *2*(5), 391–412. https://doi.org/10.64388/IREV2I5-1716082
87) Dagodzo, D., & Ahiaeke Patrick, M. C. (2021). An integrated framework for UAV, LiDAR, and GIS in infrastructure corridor management. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(5), 497–524. https://doi.org/10.32628/CSEIT217566
88) Dagodzo, D., & Ahiaeke Patrick, M. C. (2025). A framework for national-scale UAV deployment in power infrastructure: Lessons from developing economies. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(4), 779–824. https://doi.org/10.32628/CSEIT251116286
89) Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57–106. https://doi.org/10.1177/1548512920951275
90) Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*(2), 171–180. https://doi.org/10.1016/j.apergo.2013.02.009
91) Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*(744), Article 744. https://doi.org/10.3389/fpsyg.2018.00744

92) Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations*. NIST Special Publication 800-137. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137
93) Dempsey, K., Pillitteri, V., Baer, C., Niemeyer, R., Rudman, R., & Urban, S. (2020). *Assessing information security continuous monitoring (ISCM) programs: Developing an ISCM program assessment*. NIST Special Publication 800-137A. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137A
94) Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering*, *SE-13*(2), 222–232. https://doi.org/10.1109/TSE.1987.232894
95) Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. *Iconic Research and Engineering Journals*, *3*(5), 434–447. https://doi.org/10.64388/IREV3I5-1713225
96) Dosunmu, A. A., & Ogundele, P. O. (2020). Intrusion detection and prevention models for enhancing organizational cyber defense effectiveness. *Iconic Research and Engineering Journals*, *4*(6), 310–324. https://doi.org/10.64388/IREV4I6-1713226
97) Dosunmu, A. A., & Ogundele, P. O. (2021). Incident response and digital forensics strategies for rapid cyber attack containment. *Gyanshauryam, International Scientific Refereed Research Journal*, *4*(4), 239–258.
98) Dosunmu, A. A., & Ogundele, P. O. (2022). Threat intelligence integration frameworks supporting proactive enterprise cybersecurity decision making. *Gyanshauryam, International Scientific Refereed Research Journal*, *5*(3), 397–416.
99) Dosunmu, A. A., & Ogundele, P. O. (2023). Cyber threat actor analysis models for strategic enterprise security planning. *Shodhshauryam, International Scientific Refereed Research Journal*, *6*(5), 513–531.
100) Dosunmu, A. A., & Ogundele, P. O. (2024a). Breach and attack simulation frameworks for continuous validation of enterprise security controls. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(3), 1100–1119.
101) Dosunmu, A. A., & Ogundele, P. O. (2024b). Cyber risk quantification models for prioritizing enterprise security investment decisions. *International Journal of Multidisciplinary Research and Growth Evaluation*, *5*(6), 1777–1785. https://doi.org/10.54660/.IJMRGE.2024.5.6.1777-1785
102) Dosunmu, A. A., & Ogundele, P. O. (2024c). Enterprise scale continuous security validation models for regulated digital infrastructures. *International Journal of Scientific Research in Humanities and Social Sciences*, *1*(2), 929–945.
103) Dosunmu, A. A., & Ogundele, P. O. (2024d). Threat informed defence engineering models for measuring security control effectiveness at scale. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 2847–2858.
104) Dosunmu, A. A., & Ogundele, P. O. (2025a). Adversary simulation design frameworks for proactive cyber defense in complex environments. *International Journal of Computer Science and Mathematical Theory*, *11*(12), 193–209. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg193.209
105) Dosunmu, A. A., & Ogundele, P. O. (2025b). Cyber defense performance measurement frameworks for executive and board level governance. *Computer Science and IT Research Journal*, *6*(11), 895–913. https://doi.org/10.51594/csitrj.v6i11.2164
106) Dosunmu, A. A., & Ogundele, P. O. (2025c). Security orchestration and automation models for accelerating incident detection and response. *Computer Science and IT Research Journal*, *6*(11), 878–894. https://doi.org/10.51594/csitrj.v6i11.2163
107) Dosunmu, A. A., & Ogundele, P. O. (2026a). Deception based defense architectures for disrupting advanced persistent threat operations. *Engineering and Technology Journal*, *11*(1), 8475–8487. https://doi.org/10.47191/etj/v11i01.07
108) Dosunmu, A. A., & Ogundele, P. O. (2026b). Integrated threat intelligence automation and simulation models for next generation cyber defense. *Engineering and Technology Journal*, *11*(1), 8451–8462. https://doi.org/10.47191/etj/v11i01.05
109) Dosunmu, A. A., & Ogundele, P. O. (2026c). Proxy firewall and endpoint validation frameworks using breach simulation methodologies. *Engineering and Technology Journal*, *11*(1), 8463–8474. https://doi.org/10.47191/etj/v11i01.06
110) Dragos. (2025). *Dragos 2025 OT/ICS cybersecurity report: A year in review*. Dragos, Inc. https://www.dragos.com/dragos-2025-ot-cybersecurity-report-a-year-in-review
111) Ebhojie, O., Dogbatsey, E. A., & Oyeleye, A. O. (2023). Audit liaison, corrective action planning, and control compliance in multinational organisations: A systematic literature review. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2839–2850. https://doi.org/10.62225/2583049X.2023.3.6.6200
112) Efobi, O. Z., Akinleye, O. K., & Fasawe, O. (2023). Conceptual framework for developing a resilience index for post-pandemic supply chains. *Shodhshauryam, International Scientific Refereed Research Journal*, *6*(2), 421–432.
113) Ekechi, N. V., Ozowara, D. E., & Anunagba, C. O. (2026). Conceptual framework for AI governance, data privacy compliance, and financial sustainability in digital health. *Computer Science and IT Research Journal*, *7*(4), 275–299.
114) Emery, F. E., & Trist, E. L. (1965). The causal texture of organizational environments. *Human Relations*, *18*(1), 21–32. https://doi.org/10.1177/001872676501800103
115) European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
116) European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
117) European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
118) European Union Agency for Cybersecurity. (2025). *ENISA NIS360 2024: Maturity and criticality of NIS2 sectors*. https://www.enisa.europa.eu/publications/enisa-nis360-2024

119) Exec. Order No. 14028, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633 (May 17, 2021). https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
120) Eyetsemitan, R. A., Oyeleye, A. O., Ambali, K. B., & Fadayomi, O. (2022). Standard operating procedures as strategic assets in small business operations: A systematic review and implementation framework. *Gyanshauryam, International Scientific Refereed Research Journal*, *5*(2), 438–465. https://doi.org/10.32628/GISRRJ225356
121) Eze, F. I., Akinleye, O. K., & Anene, U. N. (2024). Development of a cross-border regulatory harmonization model for African pharmaceutical markets: The ARCH-Model framework. *International Journal of Health and Pharmaceutical Research*, *9*(5), 148–186. https://doi.org/10.56201/ijhpr.v9.no5.2024.pg148.186
122) Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. *Iconic Research and Engineering Journals*, *2*(12), 602–617. https://doi.org/10.64388/IREV2I12-1713779
123) Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet dossier (Version 1.4) [White paper]*. Symantec Security Response.
124) Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*(102419), Article 102419. https://doi.org/10.1016/j.jisa.2019.102419
125) Filani, O. M., Nnabueze, S. B., Ike, P. N., & Wedraogo, L. (2022). Real-time risk assessment dashboards using machine learning in hospital supply chain management systems. *International Journal of Multidisciplinary Evolutionary Research*, *3*(1), 65–76. https://doi.org/10.54660/IJMER.2022.3.1.65-76
126) Fobellah, A. N. (2025a). Cognitive biases in financial decision-making: Implications for audit and risk management in large corporations: A conceptual review. *International Journal of Science and Research Archive*, *16*(2), 17–22. https://doi.org/10.30574/ijsra.2025.16.2.2273
127) Fobellah, A. N. (2025b). Navigating digital transformation: Auditing artificial intelligence-powered financial systems: A conceptual review. *International Journal of Science and Research Archive*, *16*(2), 23–28. https://doi.org/10.30574/ijsra.2025.16.2.2274
128) Fobellah, A. N. (2025c). Unintended consequences of financial regulations: A study of corporate compliance burdens: A conceptual review. *International Journal of Science and Research Archive*, *16*(2), 29–34. https://doi.org/10.30574/ijsra.2025.16.2.2275
129) Fortinet. (2024). *2024 state of operational technology and cybersecurity report*. Fortinet, Inc. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf
130) Furnell, S. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, *2017*(2), 5–10. https://doi.org/10.1016/S1361-3723(17)30013-1
131) García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003
132) Gartner. (2023). *Gartner identifies the top 10 strategic technology trends for 2024 [Press release]*. https://www.gartner.com/en/newsroom/press-releases/2023-10-16-gartner-identifies-the-top-10-strategic-technology-trends-for-2024
133) Goddard, K., Roudsari, A., & Wyatt, J. C. (2012). Automation bias: A systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association*, *19*(1), 121–127. https://doi.org/10.1136/amiajnl-2011-000089
134) Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274
135) Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *Journal of Cybersecurity*, *6*(1), Article tyaa005. https://doi.org/10.1093/cybsec/tyaa005
136) Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011
137) Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the risk assessment maze: A meta-survey. *ACM Computing Surveys*, *51*(1), Article 11. https://doi.org/10.1145/3145905
138) Hassan, W. U., Guo, S., Li, D., Chen, Z., Jee, K., Li, Z., & Bates, A. (2019). NoDoze: Combatting threat alert fatigue with automated provenance triage. In *Proceedings of the 26th Network and Distributed System Security Symposium (NDSS 2019)*. Internet Society. https://doi.org/10.14722/ndss.2019.23349
139) Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security: A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172
140) Hussain, N., & Adebayo, A. (2026). The role of artificial intelligence in strengthening modern cybersecurity systems. *World Journal of Innovation and Modern Technology*, *10*(6), 125–181. https://doi.org/10.56201/wjimt.v10.no6.2026.pg125.181
141) Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2019). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, *21*(1), 640–660. https://doi.org/10.1109/COMST.2018.2871866
142) IBM. (2024). *Cost of a data breach report 2024*. IBM Corporation. https://www.ibm.com/reports/data-breach
143) IBM. (2025). *Cost of a data breach report 2025: The AI oversight gap*. IBM Corporation. https://www.ibm.com/reports/data-breach
144) Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, *25*(7), 498–506. https://doi.org/10.1016/j.cose.2006.03.001
145) Ike, P. N., Aifuwa, S. E., Nnabueze, S. B., Olatunde-Thorpe, J., Ogbuefi, E., Oshoba, T. O., & Akokodaripon, D. (2024). Quantitative risk architecture for public-private partnerships: A multi-layered model for allocating public and private risk. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 2669–2682. https://doi.org/10.62225/2583049X.2024.4.6.5021
146) Ike, P. N., Okojie, J. S., Nnabueze, S. B., Idu, J. O. O., Filani, O. M., & Ihwughwavwe, S. I. (2025). Digital twin-driven environmental compliance models for sustainable procurement in oil, gas, and utilities. *International Journal of Advanced Multidisciplinary Research and Studies*, *5*(5), 562–576.

147) Ilodigwe, L., & Adesemoye, A. C. (2021). The data backbone of health system transformation: A governance and architecture framework for interoperability, data quality, and advanced analytics at national scale. *International Journal of Health and Pharmaceutical Research*, *6*(2), 52–76. https://doi.org/10.56201/ijhpr.vol.6.no2.2021.pg52.76
148) Ilodigwe, L., & Adesemoye, A. C. (2024). Beyond technology: A strategic framework for building sustainable and resilient health systems through organizational strategy, operational excellence, and workforce capability. *International Journal of Medical Evaluation and Physical Report*, *8*(6), 299–319. https://doi.org/10.56201/ijmepr.v8.no6.2024.pg299.319
149) Ilodigwe, L., & Adesemoye, A. C. (2025a). Advances, risks, and implementation challenges of artificial intelligence as a force multiplier for clinical decision making and health system efficiency. *International Journal of Medical Evaluation and Physical Report*, *9*(7), 165–185. https://doi.org/10.56201/ijmepr.v9.no7.2025.pg165.185
150) Ilodigwe, L., & Adesemoye, A. C. (2025b). Executing healthcare transformation at scale: A strategic change model derived from large programs across payers, providers, and integrated health systems. *International Journal of Health and Pharmaceutical Research*, *10*(12), 253–272. https://doi.org/10.56201/ijhpr.vol.10.no12.2025.pg253.272
151) International Organization for Standardization & International Electrotechnical Commission. (2022a). *Information security, cybersecurity and privacy protection: Information security management systems: Requirements*. ISO/IEC 27001:2022. https://www.iso.org/standard/27001
152) International Organization for Standardization & International Electrotechnical Commission. (2022b). *Information security, cybersecurity and privacy protection: Guidance on managing information security risks*. ISO/IEC 27005:2022. https://www.iso.org/standard/80585.html
153) International Organization for Standardization. (2018). *Risk management: Guidelines*. ISO 31000:2018. https://www.iso.org/standard/65694.html
154) Islam, C., Babar, M. A., & Nepal, S. (2019). A multi-vocal review of security orchestration. *ACM Computing Surveys*, *52*(2), Article 37. https://doi.org/10.1145/3305268
155) Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt*. Addison-Wesley.
156) Jimoh, H. O., & Ahmed, M. O. (2024). Analyzing Network Time Protocol (NTP) based amplification DDoS attack and its mitigation techniques. *Journal of Digital Innovations and Contemporary Research in Science, Engineering and Technology*, *12*(2), 17–24. https://doi.org/10.22624/AIMS/DIGITAL/V11N2P2x
157) Jimoh, H. O., Abolle-Okoyeagu, C. J., Ahmed, M. O., & Lawal, N. O. (2023a). Advancing security in IoT-driven critical infrastructure: A focus on smart transportation system. *American Journal of Engineering Research*, *12*(12), 33–46.
158) Jimoh, H. O., Ahmed, M. O., & Fagbade, M. O. (2023b). The role of frameworks in cybersecurity governance. *Journal of Behavioural Informatics, Digital Humanities and Development Research*, *9*(4), 7–16. https://doi.org/10.22624/AIMS/BHI/V9N4P2
159) Joint Task Force Transformation Initiative. (2011). *Managing information security risk: Organization, mission, and information system view*. NIST Special Publication 800-39. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39
160) Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments*. NIST Special Publication 800-30, Rev. 1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1
161) Joint Task Force. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*. NIST Special Publication 800-37, Rev. 2. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2
162) Joint Task Force. (2020). *Security and privacy controls for information systems and organizations*. NIST Special Publication 800-53, Rev. 5. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5
163) Joint Task Force. (2022). *Assessing security and privacy controls in information systems and organizations*. NIST Special Publication 800-53A, Rev. 5. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53Ar5
164) Knight, F. H. (1921). *Risk, uncertainty and profit*. Houghton Mifflin.
165) Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002
166) Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., & Ahn, G.-J. (2019). Matched and mismatched SOCs: A qualitative study on security operations center issues. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 1955–1970). Association for Computing Machinery. https://doi.org/10.1145/3319535.3354239*Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1955–). ACM, 2019. https://doi.org/10.1145/3319535.3354239
167) Komi, N. M., & Adamolekun, A. (2021). Interpretable machine learning for early failure prediction in distributed renewable energy assets. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(6), 1015–1038. https://doi.org/10.54660/.IJMRGE.2021.2.6.1015-1038
168) Komi, N. M., & Adamolekun, A. (2022). Hierarchical, decentralized, or hybrid? A systematic review of control architectures for distributed energy resources. *International Journal of Engineering and Modern Technology*, *8*(5), 141–195. https://doi.org/10.56201/ijemt.v8.no5.2022.pg141.195
169) Komi, N. M., & Adamolekun, A. (2024). Quantifying a just transition: An econometric and skills-mapping analysis of worker displacement in the coal-to-renewable shift. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(3), 1242–1299. https://doi.org/10.32628/CSEIT25113587
170) Komi, N. M., & Adeniji, I. O. (2023). A tiered digital twin that brings predictive diagnostics to resource-constrained renewable energy sites. *International Journal of Engineering and Modern Technology*, *9*(3), 287–347. https://doi.org/10.56201/ijemt.v9.no3.2023.pg287.347

171) Komi, N. M., & Adeniji, I. O. (2024). Why energy projects survive or fail: Modeling the causal link between community trust and infrastructure durability. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 3263–3296. https://doi.org/10.62225/2583049X.2024.4.6.6459
172) Komi, N. M., & Ganiu, O. S. (2023). Edge intelligence for resilient microgrid control: Advances, energy sovereignty, and open challenges. *Gyanshauryam, International Scientific Refereed Research Journal*, *6*(3), 525–586. https://doi.org/10.32628/GISRRJ236339
173) Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139*, 156–178. https://doi.org/10.1016/j.ress.2015.02.008
174) Krumay, B., Bernroider, E. W. N., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST Cybersecurity Framework. In *Secure IT Systems: NordSec 2018* (pp. 369–384). Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-030-03638-6_23
175) Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. *Iconic Research and Engineering Journals*, *2*(6), 277–299. https://doi.org/10.64388/IREV2I6-1717205
176) Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2022a). Human-in-the-loop machine learning: A state of the art. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 656–669. https://doi.org/10.54660/.JFMR.2022.3.1.656-669
177) Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023). Active Directory attacks steps, types, and signatures. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2863–2874. https://doi.org/10.62225/2583049X.2023.3.6.6204
178) Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2024a). Integrated network and security operation center: A systematic analysis. *International Journal of Multidisciplinary Futuristic Development*, *5*(1), 65–80. https://doi.org/10.54660/IJMFD.2024.5.1.65-80
179) Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2019). Implementation of Active Directory for efficient management of enterprise networks. *Iconic Research and Engineering Journals*, *3*(4), 608–627. https://doi.org/10.64388/IREV3I4-1717206
180) Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2022b). Navigating digital transformation: Best practices for cloud migration strategies in the enterprise. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 643–655. https://doi.org/10.54660/.JFMR.2022.3.1.643-655
181) Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2024b). Keeping humans in the loop: Human-centered automated annotation with generative AI. *International Journal of Multidisciplinary Futuristic Development*, *5*(1), 81–95. https://doi.org/10.54660/IJMFD.2024.5.1.81-95
182) Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2026). On the disagreement problem in human-in-the-loop federated machine learning. *International Journal of Multidisciplinary Research and Growth Evaluation*, *7*(3), 178–192. https://doi.org/10.54660/.IJMRGE.2026.7.3.178-192
183) Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67
184) Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. E-ISAC & SANS Institute. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf
185) Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y
186) Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, *9*(20), Article 4396. https://doi.org/10.3390/app9204396
187) Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031
188) Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2020a). A review of identity and access management integration strategies in hybrid and multi cloud environments. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 795–810. https://doi.org/10.54660/.IJMRGE.2020.1.5.795-810
189) Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021). Advances in artificial intelligence techniques for secure software testing and automated regression control mechanisms. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(5), 468–496. https://doi.org/10.32628/CSEIT217565
190) Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2022a). A conceptual framework for AI enabled IT general controls and SOX audit automation processes. *Gyanshauryam, International Scientific Refereed Research Journal*, *5*(5), 384–414. https://doi.org/10.32628/GISRRJ2256239
191) Mbonu, I. S., Aliliele, C., Uzoka, E., & Oluoha, O. M. (2019a). A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. *Iconic Research and Engineering Journals*, *2*(9), 482–501. https://doi.org/10.64388/IREV2I9-1714912
192) Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020b). A conceptual framework for agile supply chain digital transformation with embedded IT risk and ISO compliance controls. *Iconic Research and Engineering Journals*, *3*(11), 566–593. https://doi.org/10.64388/IREV3I11-1714916
193) Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020c). Advances in infrastructure as code governance for secure terraform based enterprise cloud deployments. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 811–828. https://doi.org/10.54660/.IJMRGE.2020.1.5.811-828

194) Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2022b). Advances in cloud identity and access governance optimization in large scale AWS enterprise environments. *Shodhshauryam, International Scientific Refereed Research Journal*, *5*(3), 403–438. https://doi.org/10.32628/SHISRRJ225490
195) Mbonu, I. S., Iwuanyanwu, U., Uzoka, E., & Oluoha, O. M. (2019b). Advances in enterprise log analytics and automated incident response architectures using Python and SIEM platforms. *Iconic Research and Engineering Journals*, *3*(2), 1000–1019. https://doi.org/10.64388/IREV3I2-1714915
196) McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, *104*(5), 1039–1057. https://doi.org/10.1109/JPROC.2015.2512235
197) Medon, J. J., & Oduleye, T. E. (2022). A comprehensive financial reporting model for strengthening compliance and organizational accountability systems. *International Journal of Multidisciplinary Research and Growth Evaluation*, *3*(6), 768–777.
198) Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. In *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS 2018)*. Internet Society. https://doi.org/10.14722/ndss.2018.23204
199) Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195–209. https://doi.org/10.1109/JPROC.2011.2161428
200) National Cyber Security Centre. (2024). *Cyber Assessment Framework, Version 3.2*. https://www.ncsc.gov.uk/collection/cyber-assessment-framework
201) National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, Version 1.1*. NIST CSWP 6. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
202) National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. NIST AI 100-1. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
203) National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
204) Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile*. NIST Special Publication 800-61, Rev. 3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
205) Nnabueze, S. B., Ike, P. N., Olatunde-Thorpe, J., Aifuwa, S. E., Oshoba, T. O., Ogbuefi, E., & Akokodaripon, D. (2021). End-to-end visibility frameworks improving transparency, compliance, and traceability across complex global supply chain operations. *International Journal of Multidisciplinary Futuristic Development*, *2*(2), 50–60. https://doi.org/10.54660/IJMFD.2021.2.2.50-60
206) North American Electric Reliability Corporation. (2026). *NERC critical infrastructure protection roadmap*. https://www.nerc.com/globalassets/our-work/reports/special-reports/nerc_cip_roadmap_01122026.pdf
207) Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020). Advances in internal QHSE audit systems for industrial engineering operations. *Iconic Research and Engineering Journals*, *4*(4), 399–417. https://doi.org/10.64388/IREV4I4-1715499
208) Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2021). Advances in proactive hazard recognition and near miss reporting systems. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(6), 835–846. https://doi.org/10.54660/IJMRGE.2021.2.6.835-846
209) Obogo, S. F., Nwafor, M. I., & Ozobu, C. O. (2023). Conceptual leadership model for safety culture development in construction and engineering projects. *International Journal of Scientific Research in Civil Engineering*, *7*(6), 121–153. https://doi.org/10.32628/IJSRCE237554
210) Obogo, S. F., Ozobu, C. O., & Uduokhai, D. O. (2019). Advances in leadership driven safety culture transformation in large construction workforces. *Iconic Research and Engineering Journals*, *3*(5), 507–523. https://doi.org/10.64388/IREV3I5-1715497
211) Obogo, S. F., Ozobu, C. O., Garba, B. M. P., & Adio, S. A. (2026). Predictive safety analytics model for early detection of high-risk construction activities. *Global Journal of Engineering and Technology Review*, *2*(3), 92–109. https://doi.org/10.65150/EP-gjetr/V2E3/2026-03
212) Obriki, O. D., & Arumosoye, O. M. (2018). Conceptual modeling of data-driven occupational safety risk control in large-scale energy infrastructure projects. *Iconic Research and Engineering Journals*, *1*(7), 169–189. https://doi.org/10.64388/IREV1I7-1714414
213) Obriki, O. D., & Arumosoye, O. M. (2020). Conceptual framework for human error causation in high-risk construction and industrial activities. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 715–727. https://doi.org/10.54660/.IJMRGE.2020.1.5.715-727
214) Obriki, O. D., & Arumosoye, O. M. (2023). Conceptual framework for proactive hazard identification using digital safety data streams. *Gyanshauryam, International Scientific Refereed Research Journal*, *6*(3), 457–481. https://doi.org/10.32628/GISRRJ236336
215) Obriki, O. D., & Arumosoye, O. M. (2024). Systematic review of incident investigation approaches and prevention-oriented learning in industrial operations. *Shodhshauryam, International Scientific Refereed Research Journal*, *7*(4), 239–263. https://doi.org/10.32628/SHISRRJ247163
216) Obriki, O. D., Arumosoye, O. M., & Obogo, S. F. (2023). Advances in continuous hazard monitoring systems for workplace safety. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2742–2759. https://doi.org/10.62225/2583049X.2023.3.6.6075
217) Obriki, O. D., Arumosoye, O. M., & Ozobu, C. O. (2025). Conceptual model linking leading safety signals to sustained injury-free project performance. *International Journal of Scientific Research in Humanities and Social Sciences*, *2*(3), 233–254. https://doi.org/10.32628/IJSRHSS252342

218) Odejobi, O. D., Okonkwo, C. S., Ahiaeke Patrick, M. C., Okeke, O. T., & Mayo, W. (2025). AI-augmented secure software engineering: Leveraging deep learning for autonomous threat detection and mitigation. *International Journal of Engineering and Modern Technology*, *11*(12), 101–121. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg101.121
219) Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021). Conceptual model for identity-centric zero trust architecture in enterprise security governance. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(5), 393–415. https://doi.org/10.32628/IJSRCSEIT217562
220) Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., & Abolaji, T. O. (2025). Security analytics and digital forensics for enterprise risk management, advances and practical implications. *International Journal of Advanced Multidisciplinary Research and Studies*, *5*(6), 2017–2028.
221) Ogunwola, T. A., & Alozie, C. (2026). Architecting secure and compliant distributed healthcare networks: Operational approaches to health insurance portability and accountability act and health information trust alliance alignment. *International Journal of Computer Applications*, *187*(111), 1–6.
222) Ogunwola, T. A., & Deborah, F. O. (2025). Enterprise network resilience as a national security imperative: Strategies for protecting United States critical infrastructure. *International Advanced Research Journal in Science, Engineering and Technology*, *12*(10). https://doi.org/10.17148/iarjset.2025.121048
223) Ogunwole, O., Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2021). Supply chain resilience framework for critical infrastructure and gas processing plants. *Shodhshauryam, International Scientific Refereed Research Journal*, *4*(4), 444–461. https://doi.org/10.32628/SHISRRJ214462
224) Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024a). Conceptual framework for digital supply chain governance in energy and infrastructure sectors. *Gyanshauryam, International Scientific Refereed Research Journal*, *7*(4), 335–356. https://doi.org/10.32628/GISRRJ247423
225) Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024b). Framework for secure and scalable supply chain systems supporting national energy reliability. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 2816–2826. https://doi.org/10.62225/2583049X.2024.4.6.5494
226) Okonkwo, C. S., Agbabiaka, J., Okeke, O. T., & Mayo, W. (2025). Framework for national-scale supply chain optimization through integrated IT and procurement systems. *Gulf Journal of Advance Business Research*, *3*(12), 1610–1625. https://doi.org/10.51594/gjabr.v3i12.189
227) Okonkwo, C. S., Ogunwole, O., Mayo, W., & Okeke, O. T. (2021). Framework for regulatory-compliant procurement in high-risk energy environments. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(6), 595–605. https://doi.org/10.54660/IJMRGE.2021.2.6.595-605
228) Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., & Akeju, B. (2024). Enterprise cybersecurity trends and threat evolution, advances and emerging research directions. *Global Multidisciplinary Perspectives Journal*, *1*(6), 194–204. https://doi.org/10.54660/GMPJ.2024.1.6.194-204
229) Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). Conceptual model for privacy-centric security engineering in digital and cloud computing systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(5), 371–389.
230) Onche, V. O., Adegbite, M. P., & Ogbonna, C. S. (2026). Human factors in information security: A capability framework for administrative professionals in the digital workplace. *World Journal of Innovation and Modern Technology*, *10*(5), 154–179. https://doi.org/10.56201/wjimt.v10.no5.2026.pg154.179
231) Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. *International Journal of Computer Science and Mathematical Theory*, *10*(2), 117–144. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144
232) Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43–60. https://doi.org/10.1016/j.ress.2013.06.040
233) Oyeleke, A. V., Eze, F. C., & Asiedu, W. (2026). Reliability-centered maintenance strategies for minimizing downtime and maximizing performance in high-density GPU cluster environments. *International Journal of Engineering Technology Research & Management*, *10*(7), 18–38.
234) Oyeleye, A. O., Dogbatsey, E. A., & Ebhojie, O. (2025). Embedding automated close controls in public sector ERP systems: A conceptual model for audit readiness and financial reporting quality. *Zenodo.* https://doi.org/10.5281/zenodo.20097950 [Originally numbered 2(1), 110-130; journal name not captured in source.]
235) Ozowara, D. E., Adebayo, A., & Anunagba, C. O. (2022). A systematic review of cybersecurity investments and their impact on healthcare financial performance. *Shodhshauryam, International Scientific Refereed Research Journal*, *5*(1), 404–427.
236) Ozowara, D. E., Anunagba, C. O., & Adepoju, P. A. (2025). A review of ransomware economics and financial resilience strategies in hospital networks. *International Journal of Advanced Multidisciplinary Research and Studies*, *5*(6), 2284–2298. https://doi.org/10.62225/2583049X.2025.5.6.6052
237) Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors*, *52*(3), 381–410. https://doi.org/10.1177/0018720810376055
238) Pfleeger, S. L., & Cunningham, R. K. (2010). Why measuring security is hard. *IEEE Security & Privacy*, *8*(4), 46–54. https://doi.org/10.1109/MSP.2010.60

239) Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006
240) Quainoo, R., & Ogundapo, O. (2026a). A system-level power behavior model for Bluetooth and Wi-Fi coexistence in dual-mode wireless devices. *International Journal of Computer Science and Mathematical Theory*, *12*(2), 298–358. https://doi.org/10.56201/ijcsmt.vol.12.no2.2026.pg298.358
241) Quainoo, R., & Ogundapo, O. (2026b). Wireless system-on-chip performance in next-generation Internet of Things devices: A systematic review of integrated transceiver testing methodologies. *World Journal of Innovation and Modern Technology*, *10*(5), 76–126. https://doi.org/10.56201/wjimt.v10.no5.2026.pg76.126
242) Quainoo, R., Ogundapo, O., & Asiedu, W. A. (2024). Modeling the impact of impedance mismatch on wireless link performance: A framework for prototype development and system optimization. *International Journal of Computer Science and Mathematical Theory*, *10*(2), 62–116. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg62.116
243) Quainoo, R., Ogundapo, O., & Asiedu, W. A. (2025a). Predicting throughput degradation in Wi-Fi 6 networks under varying channel conditions: A physical layer performance model. *International Journal of Engineering and Modern Technology*, *11*(12), 205–264. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg205.264
244) Quainoo, R., Ogundapo, O., & Asiedu, W. A. (2025b). Test automation in wireless hardware engineering: A comprehensive review of scripting frameworks and instrument control strategies. *International Journal of Engineering and Modern Technology*, *11*(10), 405–464. https://doi.org/10.56201/ijemt.vol.11.no10.2025.pg405.464
245) Rahman, A., Parnin, C., & Williams, L. (2019). The seven sins: Security smells in infrastructure as code scripts. In *Proceedings of the 41st International Conference on Software Engineering (ICSE 2019)* (pp. 164–175). IEEE. https://doi.org/10.1109/ICSE.2019.00033
246) Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583–594. https://doi.org/10.1016/j.isatra.2007.04.003
247) Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. https://doi.org/10.1109/37.969131
248) Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture*. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
249) Ross, R., & Pillitteri, V. (2024). *Protecting controlled unclassified information in nonfederal systems and organizations*. NIST Special Publication 800-171, Rev. 3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-171r3
250) Ross, R., Winstead, M., & McEvilley, M. (2022). *Engineering trustworthy secure systems*. NIST Special Publication 800-160, Vol. 1, Rev. 1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v1r1
251) Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006
252) Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(173), Article 173. https://doi.org/10.1007/s42979-021-00557-0
253) Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*(41), Article 41. https://doi.org/10.1186/s40537-020-00318-5
254) Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792
255) Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, *14*(11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491
256) Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25
257) Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009
258) Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). *Integrating cybersecurity and enterprise risk management (ERM)*. NISTIR 8286. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286
259) Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to operational technology (OT) security*. NIST Special Publication 800-82, Rev. 3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3
260) Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). *MITRE ATT&CK: Design and philosophy (March 2020 revision)*. The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
261) Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J., & Rajagopalan, S. R. (2015). A human capital model for mitigating security analyst burnout. In *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 347–359). USENIX Association. https://www.usenix.org/conference/soups2015/proceedings/presentation/sundaramurthy
262) Sunday, E. A., Omoegun, G. O., Essien, M. A., & Oluokun, O. A. (2020). Transitioning from reactive to predictive maintenance in mechanical systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(6), 425–447.
263) Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, *10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

264) Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557–560. https://doi.org/10.1038/s42256-019-0109-1

265) Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*(4), 1836–1846. https://doi.org/10.1109/TPWRS.2008.2002298

266) Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2021). Advances in demand forecasting: Machine learning algorithms for revenue projection and financial planning accuracy. *Gyanshauryam, International Scientific Refereed Research Journal*, *4*(1), 282–317.

267) Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2024a). Advances in supply chain resilience: Predictive models for vendor risk assessment and procurement cost optimization. *International Journal of Social Sciences and Management Research*, *10*(11), 525–551. https://doi.org/10.56201/ijssmr.v10.no11.2024.pg.525.551

268) Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2024b). Real-time KPI tracking systems: A review of automated performance monitoring and data-driven decision making. *World Journal of Innovation and Modern Technology*, *8*(6), 247–281. https://doi.org/10.56201/wjimt.v8.no6.2024.pg247.281

269) Torkura, K. A., Sukmana, M. I. H., Cheng, F., & Meinel, C. (2020). CloudStrike: Chaos engineering for security and resiliency in cloud infrastructure. *IEEE Access*, *8*, 123044–123060. https://doi.org/10.1109/ACCESS.2020.3007338

270) Torkura, K. A., Sukmana, M. I. H., Cheng, F., & Meinel, C. (2021). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security*, *102*(102124), Article 102124. https://doi.org/10.1016/j.cose.2020.102124

271) Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations*, *4*(1), 3–38. https://doi.org/10.1177/001872675100400101

272) U.S. Department of Defense, Office of the Chief Information Officer. (2024). *Cybersecurity Maturity Model Certification (CMMC) model overview (Version 2.13)*. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverviewv2.pdf

273) van Ede, T., Aghakhani, H., Spahn, N., Bortolameotti, R., Cova, M., Continella, A., van Steen, M., Peter, A., Kruegel, C., & Vigna, G. (2022). DeepCASE: Semi-supervised contextual analysis of security events. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE. https://doi.org/10.1109/SP46214.2022.9833671

274) Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. *Auditing: A Journal of Practice & Theory*, *10*(1), 110–125.

275) Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems*, *13*(3), 267–281. https://doi.org/10.1016/j.accinf.2012.06.011

276) Verizon. (2024). *2024 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

277) Verizon. (2025). *2025 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

278) Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514

279) Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

280) von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

281) von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

282) Walawalkar, G., Adesuyi, M. O., Kalu, A., & Oduleye, T. E. (2025). Executive financial dashboards for real-time strategic oversight. *International Journal of Advanced Multidisciplinary Research and Studies*, *5*(6), 2042–2054.

283) Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*(5), 1344–1371. https://doi.org/10.1016/j.comnet.2012.12.017

284) Wiener, N. (1948). *Cybernetics: Or control and communication in the animal and the machine*. MIT Press.

285) World Economic Forum. (2024). *Global cybersecurity outlook 2024: Insight report*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

286) World Economic Forum. (2025). *Global cybersecurity outlook 2025: Insight report*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

287) Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950

288) Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. In *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 380–388). IEEE. https://doi.org/10.1109/iThings/CPSCom.2011.34

Corresponding Author: Chukwunenye Amadi