International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

Strengthening Telecommunications Resilience through Cybersecurity Governance, Preventive Maintenance, and Coordinated Incident Response

Josephat Deogratius Katundabwile[1], **David Mbui Kamau**[2]

School of Engineering, The Catholic University of America, Washington, DC, United States of America[1]

katundabwile@cua.edu

The Catholic University of America, Washington, DC, United States of America[2]

kamaud@cua.edu

Publication History: Received: 10.07.2026; Revised: 11.08.2026; Accepted: 15.08.2026; Published: 25.08.2026.

ABSTRACT: Telecommunications networks now underpin the delivery of financial, healthcare, government, and emergency services, which makes service continuity in this sector a matter of public as well as commercial consequence. Operators face disruption from two directions that they typically govern separately: physical and technical failure addressed through engineering maintenance, and adversarial activity addressed through information security. This article examines whether that separation is defensible and what an integrated alternative would involve. Using a structured narrative literature review of thirty peer reviewed sources, six core standards and guidance documents, and selected primary United States legal and regulatory materials, it synthesises four literatures that have developed largely in parallel, covering critical infrastructure resilience, maintenance optimisation, incident response, and cybersecurity governance. The review finds that resilience measurement weights heavily toward outcome indicators, that maintenance optimisation remains largely cyber agnostic, that incident response research centres on enterprise security operations rather than multi vendor field restoration, and that governance research is normative rather than operational. Drawing on management system logic, the governance function of the NIST Cybersecurity Framework 2.0, cyber resiliency engineering objectives, and organisational learning theory, the article proposes a thirteen stage integrated governance framework organised into phases of direction, prevention, response, and learning, together with nine performance indicators combining leading and outcome measures. Its central proposition is that preventive maintenance and security monitoring should share a governance cycle because both depend on asset inventory and behavioural baselining. The framework is proposed rather than empirically validated.

KEYWORDS: telecommunications resilience; cybersecurity governance; preventive maintenance; incident response; critical digital infrastructure; service continuity

I. INTRODUCTION

Almost everything a modern economy does passes through a telecommunications network. Payments clear over it, hospitals move imaging and records across it, emergency dispatch depends on it. The dependency has changed in kind rather than degree: telecommunications was once one utility among several and now sits underneath the others, so a transmission failure seldom stays inside the sector where it began (Owen et al., 2025). Sterbenz et al. (2010) anticipated this in arguing that communication networks need a discipline of resilience distinct from reliability engineering, because their failure modes are systemic rather than local. Virtualisation, software defined control, and IP convergence have since added failure classes with no equivalent in circuit switched environments (Bi et al., 2026).

The threat environment is now mixed. Fibre cuts, path degradation, power interruption, and equipment ageing remain the commonest causes of lost service, and they sit alongside ransomware, denial of service activity, insider misuse of privileged access, and compromise entering through supply chains (Ghadge et al., 2020). Miller et al. (2021) find that adversaries repeatedly exploit the seam where engineering practice meets information security practice, often the least

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

well governed part of the organisation. Responses have stayed divergent: preventive maintenance belongs to network engineering, cybersecurity to an information security function, and incident response is spread across a network operations centre, field crews, and external vendors, each with its own escalation path (Vielberth et al., 2020). Ahmad et al. (2020) treat this as more than inefficiency, since insight generated while handling an incident rarely reaches the functions responsible for preventing recurrence.

This article addresses one question. How can telecommunications organisations integrate cybersecurity governance, preventive maintenance, and coordinated incident response to improve service continuity and operational resilience? Its objectives are to characterise the threat environment and the costs of fragmented practice, synthesise the relevant literatures, develop an integrated governance framework, and propose indicators and implementation guidance. The contribution is integrative rather than empirical: what is missing is not evidence that governance, maintenance, and response each matter, but an account of how they interact within one operating environment and how accountability passes between them where disruption escalates.

Section 2 reviews the literature and defines key concepts. Section 3 sets out the theoretical framework, and Section 4 the methodology. Section 5 presents the synthesis, the proposed framework, and the indicator set. Section 6 discusses implications, implementation challenges, and limitations. Section 7 applies the framework to the United States context, and Section 8 concludes.

II. LITERATURE REVIEW

2.1 Key Concepts and Definitions

The literatures reviewed here use overlapping vocabulary with different meanings, so working definitions are adopted at the outset. **Critical digital infrastructure** covers the communications, computing, cloud, data, and cybersecurity systems, and the assets supporting them, on which essential services depend (Pursiainen and Kytömaa, 2023). **Cybersecurity governance** refers to the structures, decision rights, and accountability mechanisms through which an organisation directs its management of cyber risk, as distinct from the controls it deploys (Savaş and Karataş, 2022). **Operational resilience** is the capacity to anticipate, absorb, adapt to, and recover from disruption while continuing to deliver critical services; Galaitsi et al. (2023) separate it from business continuity management, which concerns pre planned maintenance of defined activities during interruption. **Engineering risk management** is the systematic identification, assessment, and treatment of technical failure modes affecting network assets (Aghazadeh Ardebili et al., 2024). **Preventive maintenance** is maintenance performed at set intervals or against prescribed criteria to reduce the likelihood of failure or degradation, including condition based and predictive variants (Pinciroli et al., 2023). **Coordinated incident response** covers preparation, detection, analysis, containment, eradication, recovery, and post incident activity conducted across internal functions and external parties under a single command structure (National Institute of Standards and Technology [NIST], 2025). **Service continuity**, the sustained delivery of a defined service at an agreed performance level, is treated here as the outcome resilience arrangements exist to protect (Steen et al., 2024).

2.2 Telecommunications as Critical Digital Infrastructure

Designating a sector as critical is a statement about consequence rather than size. Pursiainen and Kytömaa (2023) trace through European policy a shift from protecting discrete assets toward sustaining the resilience of critical entities and the services they deliver. The vocabulary matters: protecting an asset invites a posture built on perimeters and physical integrity, while sustaining a service invites one built on continuity of function, a more demanding standard. Owen et al. (2025) describe the same movement in engineering terms, arguing that telecommunications now underpins what they call sovereign functions.

The dependency is visible when services are traced to their transport layer. Cloud computing has concentrated processing and storage in few facilities, so value reaches the user only if the network path holds; financial authorisation and settlement are time sensitive enough that brief interruption is materially costly; and healthcare imaging, records, and connected monitoring all assume a network that is present. Public safety communications warrant separate treatment because failure is measured differently there, since dispatch, responder coordination, and alerting depend on availability at exactly the moments networks are most stressed. The Cybersecurity and Infrastructure Security Agency ([CISA], n.d.) built its Public Safety Communications and Cyber Resiliency Toolkit on this premise. Jiang et al. (2025) find national emergency management arrangements uneven, separating two things often conflated: a network can be technically capable of surviving disruption while the arrangements governing restoration remain unclear. Gallarno et al. (2024) reach a compatible conclusion from the engineering side, showing resilience must be specified as a design requirement and assessed against defined scenarios rather than assumed to follow from component reliability.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

Two structural features compound the exposure. Bi et al. (2026) note that virtualised functions, shared transport routes, and centralised control planes mean the logical independence users perceive often does not exist at the physical or control layer, so redundancy that exists on paper can fail to exist in practice. And the direction of dependency is asymmetric, since energy, water, and transport depend on telecommunications for monitoring and control while it depends chiefly on energy. Patriarca et al. (2022), modelling cyber resilience in water treatment and distribution, show how disruption to the communications and control layer becomes loss of physical process capability, and how recovery of the physical function depends on restoring the informational one first; that study is cited for the mechanism, not as evidence about telecommunications outages.

The implication is definitional. If criticality derives from the services depending on the network, the relevant measure of resilience is service continuity as those dependants experience it, not equipment availability as the operator records it, a distinction supported by Galaitsi et al. (2023) and Steen et al. (2024). Aghazadeh Ardebili et al. (2024) find the field of cyber resilience assessment methodologically diverse but institutionally underdeveloped, with assessment practice ahead of the governance needed to act on its results.

2.3 Cyber and Operational Threats

Operators conventionally sort threats into operational causes, which interrupt transmission physically, and cyber threats involving a deliberate adversary. The categories carry organisational weight because they map onto different departments and reporting lines, but the distinction is hard to sustain. Sterbenz et al. (2010) argued for a single taxonomy spanning natural faults, environmental conditions, human error, and malicious attack, since the network experiences all of them as loss of function. Bi et al. (2026) reach a similar position from contemporary architectures, where a misconfigured orchestration function and a compromised one produce similar symptoms at the transport layer.

On the operational side, fibre damage is widely reported as a leading cause of significant transmission loss in terrestrial networks, and the commonly cited causes are mundane: excavation and construction, road and rail projects, agricultural activity, and cable theft (Owen et al., 2025). Route diversity is the standard mitigation, though separately provisioned services often share physical routes somewhere along their path (Owen et al., 2025). Hardware degradation operates on a different timescale and is what preventive maintenance exists to address, since transmission equipment, radio units, power systems, and cooling plant deteriorate gradually and to a useful extent predictably (Pinciroli et al., 2023). Environmental hazards act through both direct damage and dependency failure, since extended power interruption removes the energy every other component needs (Jiang et al., 2025). Software failure and human error cross the categorical boundary directly, since configuration errors and defects in management software have caused substantial outages with no adversary involved, and the same mechanisms are what an adversary exploits when one is. Vielberth et al. (2020) identify separating anomalous behaviour with operational causes from anomalous behaviour with hostile ones as a persistent open challenge.

On the adversarial side, the significance of ransomware is that its usual targets are not the transmission network. Business and operational support systems, provisioning platforms, and management infrastructure are what gets encrypted, so an operator can lose the ability to provision, bill, monitor, or dispatch while equipment carries traffic normally, and continuity as customers experience it degrades without a single transmission fault. Denial of service activity attacks availability directly, and operators face it doubly, as targets and as the transit path for attacks on customers. Insider threat is structurally significant because network operations roles require the ability to reconfigure paths, alter thresholds, and reach management systems, capabilities indistinguishable from those an attacker seeks, which makes access control, separation of duties, and logging the governing response rather than detection alone. On supply chain compromise, Ghadge et al. (2020) argue that risk assessment practice has not kept pace with the interconnection it is meant to assess, and telecommunications is exposed through vendor firmware updates, managed service providers, and field subcontractors. Wallis and Dorey (2023) find contractual arrangements insufficient alone, with resilience depending on sustained collaboration between operator and supplier, while Miller et al. (2021) document how adversaries exploit the operational and information technology boundary.

Three differences between the categories determine what defensive posture is appropriate. The first is predictability: operational failures are broadly stochastic and statistically stationary, so historical rates carry predictive value, which is what makes interval based maintenance work, whereas an adversary observes defences and adapts. Aghazadeh Ardebili et al. (2024) note this is what complicates cyber resilience assessment, since methods inherited from reliability engineering assume a threat that does not respond to the assessment. The second is detectability: physical failure announces itself through alarms and traffic loss, while compromise is designed to remain undetected, and the resulting asymmetry between occurrence and discovery has direct implications for measurement. The third is recurrence:

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

operational faults repeat by location, whereas cyber incidents recur by technique or exposure class. Saeed et al. (2023) argue that learning here depends on external intelligence sharing to a degree operational fault analysis does not, and Busetti and Scanni (2025) find that the collective learning value of incident reporting depends on how reporting obligations are designed.

2.4 Limitations of Fragmented Maintenance and Incident Response

Fragmentation is rarely a design decision. It accumulates as functions are added, outsourced, or reorganised, and its costs surface only under disruption. Four mechanisms recur in the literature. The first is loss of shared situational awareness: Ahmad et al. (2021) show effective response depends on a common operational picture assembled across roles, which degrades when the parties holding its components report separately. The second is delayed escalation and unclear ownership, since where authority to declare an incident or dispatch a vendor sits in different places, time is lost to negotiation rather than diagnosis. Staves et al. (2022) argue that frameworks for critical infrastructure must specify decision rights explicitly, because restoration depends on parties the operator does not command. The third is vendor fragmentation, as multi vendor environments distribute technical knowledge across organisations with separate contractual obligations, and Wallis and Dorey (2023) find contracts alone do not produce coordinated response. The fourth is inconsistent documentation, which converts a coordination problem into a learning problem. Patterson et al. (2023) find learning frequently blocked by incomplete records, and Ahmad et al. (2020) show insight generated during response rarely reaches the functions that could prevent recurrence.

2.5 Cybersecurity Governance

Governance contributes something controls cannot: it allocates decision rights and fixes accountability before disruption occurs. Savaş and Karataş (2022) frame cybersecurity governance as the direction and oversight of cyber risk management rather than its execution. Two authoritative instruments structure current practice. The NIST Cybersecurity Framework 2.0 raised governance to a Function in its own right, placing organisational context, risk strategy, roles and responsibilities, policy, and oversight alongside the operational functions of identification, protection, detection, response, and recovery (NIST, 2024). ISO/IEC 27001 approaches the same problem through a certified management system requiring documented risk ownership, defined treatment decisions, and periodic review (International Organization for Standardization [ISO], 2022). Culot et al. (2021) caution that certification and substantive security are not the same, since organisations vary considerably in whether the management system drives decisions or documents them after the fact.

For telecommunications, the governance question that matters most is scope. If risk ownership is defined only over information systems, engineering decisions about maintenance intervals, spares holdings, route diversity, and equipment replacement fall outside the risk governance structure entirely, even though they determine exposure to the operational failures causing most lost service. Maturity models offer staged improvement (Büyüközkan and Güler, 2025), though maturity measures process consistency rather than resilience achieved.

2.6 Preventive Maintenance

Preventive maintenance is usually justified on availability and cost grounds, but its contribution to resilience is broader and rests on the premise, central to condition based and predictive maintenance, that many failure modes are preceded by observable change in measurable parameters (Pinciroli et al., 2023). Pinciroli et al. (2023) trace the movement toward condition based and predictive approaches in which intervention is triggered by observed asset state rather than elapsed time. For transmission networks the relevant parameters are already collected by network management systems, and analysis of received signal level, transmit power, interference, and hardware operating temperature allows degradation to be identified while it is still degradation rather than outage. Risk based prioritisation then determines which findings warrant field inspection.

Three connections to cybersecurity follow, and they are why preventive maintenance belongs inside a security governance framework rather than beside it. Maintenance programmes sustain the asset inventory on which the Identify function of the Cybersecurity Framework depends (NIST, 2024). Condition monitoring establishes the behavioural baseline anomaly detection requires, since both disciplines need to know what normal looks like for an asset. And firmware and software currency, a maintenance activity by convention, determines vulnerability exposure directly.

2.7 Coordinated Incident Response

Incident response guidance has recently been restructured around governance rather than sequence. NIST SP 800-61 Revision 3 organises its recommendations through the Cybersecurity Framework 2.0 Functions, replacing the standalone lifecycle of earlier revisions and integrating response into risk management as a continuing activity (NIST,

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

2025). The practical implication is that preparation is not a phase completed before incidents but a governance obligation maintained between them.

The operational sequence nonetheless remains recognisable: preparation establishes plans, roles, and tooling; detection and analysis determine what has occurred; containment limits propagation, eradication removes the cause, and recovery restores service to objectives ISO 22301 expresses as recovery time and recovery point targets agreed in advance rather than negotiated during disruption (ISO, 2019). Post incident activity converts the event into organisational knowledge.

Two aspects deserve emphasis for telecommunications. The first is situational awareness, where Naseer et al. (2021) and Naseer, Desouza, et al. (2024) find real time analytics contribute to response agility by shortening the interval between observation and decision. The second is multi vendor coordination, the defining feature of restoration in this sector and the weakest point in most response arrangements, since restoration typically requires action by equipment vendors, subcontractors, and infrastructure owners, none of whom report to the operator's incident commander. Post incident learning completes the cycle and is where it most often breaks (Patterson et al., 2023).

III. THEORETICAL FRAMEWORK

Four established positions provide the theoretical basis for the integration this article proposes, and each supplies a different component of the eventual structure.

The first is management system theory, expressed operationally in the plan, do, check, act cycle underlying both ISO/IEC 27001 and ISO 22301 (ISO, 2019, 2022). Its relevance is that it treats control as continuous rather than episodic, requiring that performance be reviewed and that review revise the plan. Applied here, it supplies the cyclical rather than linear form of the framework and the requirement that learning return to direction.

The second is the governance centred model of the Cybersecurity Framework 2.0, in which governance is not one activity among six but the Function through which organisational context, risk strategy, roles, and policy are established for all others (NIST, 2024). This supports placing accountability at the head of the cycle rather than alongside operational activity, and it is the theoretical warrant for treating scope of risk ownership, rather than control selection, as the primary governance question.

The third is cyber resiliency engineering, which specifies four objectives for systems operating in contested environments: anticipating adverse conditions, withstanding them, recovering from them, and adapting afterwards (NIST, 2021). These objectives are useful here because they are stated independently of threat origin, which matches the finding in Section 2.3 that operational and adversarial disruption converge on the same outcome. They provide the four phase structure into which the framework's stages are grouped.

The fourth is organisational learning theory applied to security. Ahmad et al. (2020) demonstrate that knowledge generated during incident response becomes organisational value only where mechanisms exist to transfer it to preventive functions, and Naseer, Desouza, et al. (2024) frame the recycling of such insight as a dynamic capability rather than a procedural step. This supplies the framework's return path and the argument that root cause analysis and corrective action are governance activities rather than closure formalities.

Taken together these positions yield a testable proposition: that resilience outcomes improve where prevention and detection share a governance cycle, because both depend on the same underlying knowledge of asset state, and where accountability for that cycle is assigned before disruption rather than negotiated during it.

IV. METHODOLOGY

4.1 Design

This study employs a structured narrative literature review followed by conceptual framework development. A narrative approach was selected over a systematic review because the research question is integrative rather than effect estimating: it asks how the four bodies of knowledge identified in Section 5.1 relate to one another, not whether an intervention produces a measured outcome. The review is structured in that source selection, thematic organisation, and synthesis followed the criteria below, but no claim is made to the exhaustiveness or reproducibility of a systematic review, and no meta analysis was performed.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

4.2 Source Selection

The corpus comprises thirty peer reviewed sources, six core standards and guidance documents, and selected primary United States legal and regulatory materials cited in Section 7. Peer reviewed sources were selected across four thematic domains corresponding to the four literatures synthesised in Section 5.1: critical infrastructure resilience and telecommunications network reliability, maintenance engineering and optimisation, incident response and organisational learning, and cybersecurity governance and maturity. Selection prioritised publications from 2019 onward to reflect current architectures and threat conditions, with earlier work retained where foundational, as with Sterbenz et al. (2010). Preference was given to systematic reviews and surveys where available, since these consolidate larger bodies of primary work than a narrative review could examine directly.

The standards corpus comprises NIST Special Publications 800-61 Revision 3 and 800-160 Volume 2 Revision 1, the Cybersecurity Framework 2.0, ISO/IEC 27001:2022, ISO 22301:2019, and the CISA Public Safety Communications and Cyber Resiliency Toolkit. These were included because governance and response practice in this sector is shaped by authoritative guidance as much as by research literature.

4.3 Synthesis and Framework Development

Sources were organised thematically rather than chronologically, and synthesis proceeded by identifying where the domains address the same operational problem in different vocabulary and where each is silent on matters the others treat as central. Points of silence rather than agreement drove framework development, since the contribution sought was integration across gaps. Framework stages were derived from activities the reviewed literature and standards treat as necessary, and sequenced according to the theoretical positions in Section 3.

4.4 Use of Practitioner Insight

Practitioner observation from transmission network operations informed the identification of coordination problems in Section 2.4 and maintenance practice in Section 2.6. It is used illustratively and reported in anonymised form without organisational identifiers, restoration times, performance statistics, customer information, or proprietary procedures. It constitutes neither primary data nor empirical validation, and no analytical claim rests on it.

4.5 Methodological Limitations

Three limitations follow. Narrative selection carries a bias risk that systematic protocols reduce, and while thematic breadth was pursued deliberately, exhaustiveness cannot be claimed. The framework is conceptual and unmeasured, so its components rest on argument rather than outcome data. And reliance on review articles for domain coverage means the synthesis inherits their limitations.

V. RESULTS

5.1 Synthesis of the Literature

The review identifies four bodies of work bearing on telecommunications resilience that have developed largely in parallel, each substantial within its own boundaries and each silent on matters the others treat as central.

Critical infrastructure resilience research has produced extensive conceptual and measurement work (Mottahedi et al., 2021; Osei-Kyei et al., 2023; Sathurshan et al., 2022), yet seldom treats maintenance execution or vendor coordination as measurable determinants, and its indicators are weighted toward outcomes, describing how a system behaved rather than the practices determining how it will behave next time. Maintenance optimisation research has advanced considerably (Pinciroli et al., 2023) but remains largely cyber agnostic, modelling failure as stochastic rather than possibly adversarial, which matters because the assumption of stationarity that makes interval based maintenance work does not hold against an adversary that adapts. Incident response research offers developed insight into response agility and analytics enabled capability (Naseer et al., 2021; Naseer, Desouza, et al., 2024), though centred on the enterprise security operations centre rather than the multi vendor field restoration characteristic of transmission networks, where the parties determining restoration time do not report to the operator. Cybersecurity governance and maturity research supplies normative structures for oversight (Culot et al., 2021; Büyüközkan and Güler, 2025) without specifying how they connect to engineering maintenance cycles, leaving the scope problem identified in Section 2.5 unaddressed.

The synthesis therefore identifies an integrative gap: what is absent is not evidence that governance, maintenance, and response each contribute to resilience, but an account of how they interact within one operating environment and how accountability transfers between them where disruption escalates.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

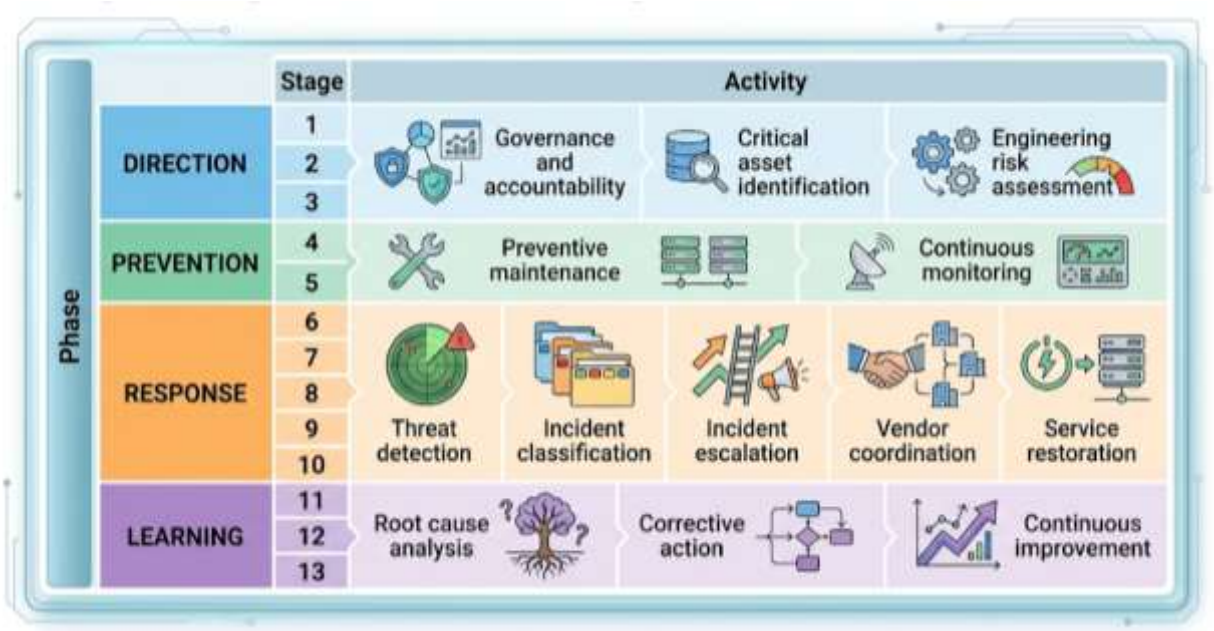
DOI:10.15662/IJEETR.2026.0804009

5.2 The Proposed Integrated Governance Framework

The framework connects the reviewed components into a single cycle, presented in Figure 1.

Figure 1

Integrated Telecommunications Cyber Resilience Governance Framework



Note. Source: Developed by the authors. Stages proceed in sequence from 1 to 13, and stage 13 returns to stage 1, so the framework is cyclical rather than terminating: continuous improvement revises asset criticality, risk assessment, and maintenance priorities at the direction phase. Alternative text: a table of thirteen numbered governance stages grouped into four phases named direction, prevention, response, and learning, with a return path from stage 13 to stage 1 forming a closed cycle.

The thirteen stages form four phases corresponding to the cyber resiliency objectives set out in Section 3.

Direction, corresponding to anticipation. Governance and accountability establish decision rights, risk ownership, and escalation authority spanning engineering and information security, addressing the scope problem in Section 2.5. Critical asset identification maps services to the assets delivering them, so criticality is defined by service consequence rather than asset value. Engineering risk assessment then prioritises failure modes across physical, technical, and adversarial causes in a common register rather than separate ones.

Prevention, corresponding to withstanding. Preventive maintenance acts on prioritised engineering risk, with intervals and methods set by asset criticality rather than applied uniformly. Continuous monitoring maintains the behavioural baseline serving both condition assessment and anomaly detection, which is the point at which the two monitoring disciplines share infrastructure rather than duplicating it.

Response, corresponding to recovery. Threat detection covers operational and adversarial causes without requiring origin to be known in advance, since the two are often indistinguishable at onset. Classification assigns severity by service consequence, escalation follows pre agreed authority thresholds, vendor coordination operates under unified command with decision rights defined before the incident, and restoration proceeds against continuity objectives set in advance.

Learning, corresponding to adaptation. Root cause analysis addresses technical and organisational causes together, corrective actions are tracked to closure with named ownership, and continuous improvement returns findings to governance, where they revise asset criticality, risk assessment, and maintenance priorities, closing the cycle.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

The framework's distinguishing feature is that preventive maintenance and security monitoring occupy a single governance cycle rather than running in parallel, justified by their common dependence on asset inventory and behavioural baselining.

5.3 Proposed Performance Indicators

Indicators should measure the operating practices that produce resilience alongside the outcomes that reveal it, addressing the outcome weighting identified in Section 5.1. Table 1 sets out the proposed set.

Table 1

Proposed Telecommunications Resilience Performance Indicators

Indicator	Function
Service availability	Outcome measure defined at service rather than element level, consistent with continuity as the protected outcome
Mean time between failures	Asset reliability trend, informing maintenance interval and replacement decisions
Mean time to detect	Interval between occurrence and awareness; the measure most sensitive to the detection asymmetry described in Section 2.3
Mean time to restore	Response and coordination effectiveness once an incident is known
Preventive maintenance completion rate	Whether prevention is executed as planned; a leading indicator against outcome measures that lag
Vendor response time	Performance of the external parties on whom restoration depends
Escalation time	Whether governance thresholds function under pressure or are bypassed
Repeat failure rate	Whether corrective action addressed cause or symptom
Corrective action closure rate	Integrity of the learning loop closing the framework cycle

Note. Source: Developed by the authors.

Read in combination these indicators expose specific failure patterns. High availability with a low maintenance completion rate suggests resilience is being sustained by margin rather than management. A short restoration time with a long detection time indicates capable response applied late. A rising repeat failure rate alongside a high closure rate indicates actions are being closed without resolving cause.

VI. DISCUSSION

6.1 Interpretation

The synthesis supports a specific reading of why fragmentation persists. It is not principally a failure of technical capability or individual competence but a consequence of how risk ownership is scoped. Where governance defines ownership over information systems alone, decisions with the largest bearing on service continuity, namely maintenance intervals, spares holdings, route diversity, and equipment replacement, sit outside the risk governance structure while remaining formally accounted for elsewhere. Each function can therefore discharge its responsibilities correctly while the organisation remains exposed.

This reframes what integration requires. The framework does not ask engineering and security functions to merge, which would be neither practical nor desirable given the different expertise each requires. It asks that they share a governance cycle, a common risk register, and defined points of accountability transfer, which is a governance change rather than an organisational restructuring.

The proposition that preventive maintenance and security monitoring share a technical foundation is the element most open to challenge. If their common dependence on knowing what normal looks like for an asset holds in operating environments, integration should yield measurable benefit in detection intervals; if not, the two may be better served by coordination at the governance layer alone.

6.2 Implementation Challenges

Adoption is constrained more by organisational conditions than technical ones. Resistance is likely where the framework redistributes authority, and staged adoption using maturity levels offers a less confrontational route than wholesale restructuring (Büyüközkan and Güler, 2025). Budget constraints bear on prevention disproportionately, since

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

preventive investment competes against visible restoration costs while its benefits appear as absent incidents, which is part of the argument for leading indicators. Legacy infrastructure limits what monitoring can observe, as equipment predating current management interfaces may not support the telemetry assumed here (Miller et al., 2021), making partial implementation prioritised by asset criticality more realistic than deferral. Workforce capability constrains adoption, since the framework requires staff who can read both engineering and security signals, and cross functional incident review is a practical development mechanism. Governance maturity determines how much is usable at once, and organisations without functioning risk ownership should establish it first, particularly given the caution of Culot et al. (2021) that formal compliance can substitute for substantive practice. Regulatory divergence complicates multi jurisdiction operation where reporting obligations differ (Busetti and Scanni, 2025; Pursiainen and Kytömaa, 2023), and vendor interoperability remains an obstacle, since management systems rarely share data models (Wallis and Dorey, 2023).

6.3 Limitations

Beyond the methodological limitations noted in Section 4.5, the framework is proposed rather than validated, and no claim is made that it has produced measured improvement in any operating environment. The indicator set is likewise proposed on analytical grounds rather than calibrated against operational data, so thresholds would need to be established locally. Its applicability beyond transmission network operations, from which the illustrative practitioner material derives, has not been examined.

VII. APPLICATION TO THE UNITED STATES CONTEXT

The framework's practical value depends on the regulatory environment in which it operates. The United States presents a case in which the institutional structure reproduces, at the level of federal oversight, the same separation between operational and cyber disruption that this article identifies as a weakness within operators.

7.1 Two Reporting Regimes, Two Definitions of an Incident

Communications is one of the sixteen critical infrastructure sectors designated under National Security Memorandum 22, which superseded Presidential Policy Directive 21 in April 2024 and reaffirmed both the sector designations and the sector risk management agency structure (White House, 2024). Providers are subject to two distinct reporting regimes with different triggers, timetables, and recipients.

Operational disruption is governed by Part 4 of the Federal Communications Commission's rules (47 C.F.R. pt. 4), under which covered providers report outages meeting defined duration and magnitude thresholds through the Network Outage Reporting System, with additional provisions for disruptions affecting 911 facilities, special offices and facilities, and certain airports (Federal Communications Commission, n.d.). Reporting obligations are keyed to measurable service impact rather than to cause. Parallel arrangements cover disaster conditions through the Disaster Information Reporting System, reporting in which became mandatory for covered providers on activation under rules adopted in 2024 (47 C.F.R. § 4.18; Federal Communications Commission, 2024), and coordinated restoration through the Mandatory Disaster Response Initiative, which requires participating wireless providers to provide roaming where technically feasible and to maintain mutual aid arrangements when triggered by activation of Emergency Support Function 2, activation of the Disaster Information Reporting System, or a state request (47 C.F.R. § 4.17).

Cyber disruption is governed separately. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 directs the Cybersecurity and Infrastructure Security Agency to require covered entities to report covered cyber incidents within 72 hours and ransomware payments within 24 hours (Cyber Incident Reporting for Critical Infrastructure Act of 2022). The agency published a notice of proposed rulemaking in April 2024 (Cybersecurity and Infrastructure Security Agency, 2024). The reporting requirements are not yet in force and will take effect only when the final rule does; the agency's own guidance states that reporting under the Act is not presently required (Cybersecurity and Infrastructure Security Agency, n.d.). Because the timetable has moved more than once, the status of the final rule should be reverified immediately before publication.

The consequence for operators is structural. The same disruption may be reportable under one regime, both, or neither, depending on whether it is characterised by service impact or by cause, and the two determinations are made against different criteria on different clocks. An operator whose internal functions are separated along the same line will make those determinations twice, in two places, from two partial views of the event. This is precisely the condition the incident classification stage of the proposed framework addresses, by assigning severity from service consequence first and mapping that single assessment onto each applicable reporting obligation.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

7.2 The Weight Carried by Internal Governance

Recent regulatory history sharpens the point. Following the Salt Typhoon intrusions reported in late 2024 to have affected multiple United States communications companies, the Commission adopted a declaratory ruling in January 2025 holding that section 105 of the Communications Assistance for Law Enforcement Act obliges carriers to secure their networks against unlawful access, accompanied by a notice of proposed rulemaking on cybersecurity risk management requirements. On 20 November 2025 the Commission adopted an order on reconsideration rescinding that ruling, finding that it had misconstrued the statute, and withdrawing the associated proposed rulemaking in favour of a targeted and collaborative approach (Federal Communications Commission, 2025).

The result is that United States communications providers operate under several incident reporting and sector specific requirements, but no single generally applicable federal cybersecurity risk management mandate covers every communications provider. Authoritative guidance in the form of the Cybersecurity Framework 2.0 (NIST, 2024) and the CISA Cross-Sector Cybersecurity Performance Goals remains available, and the performance goals are explicitly voluntary, carrying no certification and no conferred status (Cybersecurity and Infrastructure Security Agency, 2025). Internal governance therefore carries the weight that regulation does not, which strengthens rather than weakens the case for the framework advanced here: where external certification of risk management practice is absent, the indicator set proposed in Section 5.3 supplies the internal evidence that prevention, escalation, and corrective action are functioning, and the governance stage supplies the accountability that certification would otherwise impose.

VIII. CONCLUSION

This article has argued that telecommunications resilience depends on integration between functions most operators govern separately. The review found four literatures developing in parallel, with resilience measurement weighted toward outcomes, maintenance optimisation largely cyber agnostic, incident response research centred on enterprise security operations, and governance research normative rather than operational. The framework proposed here connects them through a single cycle in which accountability is established before disruption and learning returns to governance after it, supported by an indicator set combining leading and outcome measures.

The contribution is integrative. Its central proposition, that preventive maintenance and security monitoring should share a governance cycle because they share a dependence on asset inventory and behavioural baselining, is testable and would benefit from testing. Three directions follow. Empirical evaluation in operating environments would establish whether integration produces the effects proposed. Comparative work across regulatory regimes would clarify how reporting obligations shape learning. And development of leading indicators for resilience, as distinct from outcome measures, remains an open requirement in the measurement literature.

AUTHOR CONTRIBUTIONS

J. D. Katundabwile: conceptualisation; methodology; investigation; formal analysis; development of the integrated governance framework and performance indicator set; provision of the transmission network operations domain expertise informing Sections 2.4 and 2.6; writing of the original draft. **D. M. Kamau:** validation; verification of literature and standards sources; writing, review, and editing; critical revision of the framework structure. Both authors have read and approved the final manuscript and accept responsibility for its content.

REFERENCES

1. Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. *Applied Sciences*, *14*(24), 11807. https://doi.org/10.3390/app142411807

2. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

3. Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

4. Bi, S., Yuan, X., Hu, S., Li, K., Ni, W., Hossain, E., & Wang, X. (2026). Resilience and failure analysis in next-generation communication networks: A contemporary survey. *IEEE Transactions on Network Science and Engineering*, *13*, 2793–2821. https://doi.org/10.1109/tnse.2025.3620950

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

5. Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity: From threat detection to policy learning. *Government Information Quarterly, 42*(1), 102000. https://doi.org/10.1016/j.giq.2024.102000
6. Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. *Technological Forecasting and Social Change, 213*, 123996. https://doi.org/10.1016/j.techfore.2025.123996
7. 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
8. Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 49, 1038 (2022) (codified at 6 U.S.C. §§ 681–681g).
9. Cybersecurity and Infrastructure Security Agency. (n.d.). *Public safety communications and cyber resiliency toolkit* (Version 24.2). Retrieved August 6, 2026, from https://www.cisa.gov/resources-tools/resources/communications-and-cyber-resiliency-toolkit
10. Cybersecurity and Infrastructure Security Agency. (2024). *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) reporting requirements: Notice of proposed rulemaking* (89 Fed. Reg. 23644, April 4, 2024). https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements
11. Cybersecurity and Infrastructure Security Agency. (2025). *Cross-sector cybersecurity performance goals.* https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
12. Cybersecurity and Infrastructure Security Agency. (n.d.). *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA): Frequently asked questions.* Retrieved August 19, 2026, from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/circia/faqs
13. Federal Communications Commission. (2024). *Resilient networks; disruptions to communications* (Second Report and Order, FCC 24-5; 89 Fed. Reg. 25542, April 11, 2024). https://www.federalregister.gov/documents/2024/04/11/2024-07402/resilient-networks-disruptions-to-communications
14. Federal Communications Commission. (2025). *Protecting the nation's communications systems from cybersecurity threats* (Order on Reconsideration, PS Docket No. 22-329, FCC 25-81; 90 Fed. Reg. 58006, December 15, 2025). https://www.federalregister.gov/documents/2025/12/15/2025-22830/protecting-the-nations-communications-systems-from-cybersecurity-threats
15. Federal Communications Commission. (n.d.). *Network Outage Reporting System (NORS).* Retrieved August 19, 2026, from https://www.fcc.gov/general/network-outage-reporting-system-nors
16. Galaitsi, S. E., Pinigina, E., Keisler, J. M., Pescaroli, G., Keenan, J. M., & Linkov, I. (2023). Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis. *International Journal of Disaster Risk Science, 14*(5), 713–721. https://doi.org/10.1007/s13753-023-00494-x
17. Gallarno, G., Muniz, J., Parnell, G. S., Pohl, E. A., & Wu, J. (2024). Development and assessment of a resilient telecoms system. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 21*(4), 405–420. https://doi.org/10.1177/15485129221143791
18. Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal, 25*(2), 223–240. https://doi.org/10.1108/scm-10-2018-0357
19. International Organization for Standardization. (2019). *ISO 22301:2019. Security and resilience: Business continuity management systems, requirements.*
20. International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection: Information security management systems, requirements.*
21. Jiang, P., Rowsell, J., & Schmidt, S. (2025). Crisis-ready telecom: Global approaches to emergency management in telecommunications. *Telecommunications Policy, 49*(4), 102914. https://doi.org/10.1016/j.telpol.2025.102914
22. Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection, 35*, 100464. https://doi.org/10.1016/j.ijcip.2021.100464
23. Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. (2021). The resilience of critical infrastructure systems: A systematic literature review. *Energies, 14*(6), 1571. https://doi.org/10.3390/en14061571
24. Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management, 59*, 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334
25. Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & Security, 135*, 103525. https://doi.org/10.1016/j.cose.2023.103525

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804009

26. Naseer, H., Desouza, K. C., Maynard, S. B., & Ahmad, A. (2024). Enabling cybersecurity incident response agility through dynamic capabilities: The role of real-time analytics. *European Journal of Information Systems, 33*(2), 200–220. https://doi.org/10.1080/0960085x.2023.2257168
27. National Institute of Standards and Technology. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). https://doi.org/10.6028/NIST.SP.800-160v2r1
28. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). https://doi.org/10.6028/NIST.CSWP.29
29. National Institute of Standards and Technology. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61, Rev. 3). https://doi.org/10.6028/NIST.SP.800-61r3
30. Osei-Kyei, R., Almeida, L. M., Ampratwum, G., & Tam, V. (2023). Systematic review of critical infrastructure resilience indicators. *Construction Innovation, 23*(5), 1210–1231. https://doi.org/10.1108/ci-03-2021-0047
31. Owen, R., Bryant, A., Finch, L., Franklin, D., Abdollahi, M., & Abolhasan, M. (2025). Failures and resilience in the IP era: Navigating the fragility of modern telecommunications networks: The sovereign functions. *IEEE Access, 13*, 155759–155777. https://doi.org/10.1109/access.2025.3602054
32. Patriarca, R., Simone, F., & Di Gravio, G. (2022). Modelling cyber resilience in a water treatment and distribution system. *Reliability Engineering & System Safety, 226*, 108653. https://doi.org/10.1016/j.ress.2022.108653
33. Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security, 132*, 103309. https://doi.org/10.1016/j.cose.2023.103309
34. Pinciroli, L., Baraldi, P., & Zio, E. (2023). Maintenance optimization in industry 4.0. *Reliability Engineering & System Safety, 234*, 109204. https://doi.org/10.1016/j.ress.2023.109204
35. Pursiainen, C., & Kytömaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure, 8*(sup1), 85–101. https://doi.org/10.1080/23789689.2022.2128562
36. Reporting Requirements for Disruptions to Communications, 47 C.F.R. pt. 4 (2025).
37. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273
38. Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures, 7*(5), 67. https://doi.org/10.3390/infrastructures7050067
39. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4
40. Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A cyber incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection, 37*, 100505. https://doi.org/10.1016/j.ijcip.2021.100505
41. Steen, R., Haug, O. J., & Patriarca, R. (2024). Business continuity and resilience management: A conceptual framework. *Journal of Contingencies and Crisis Management, 32*(1), e12501. https://doi.org/10.1111/1468-5973.12501
42. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks, 54*(8), 1245–1265. https://doi.org/10.1016/j.comnet.2010.03.005
43. 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
44. Wallis, T., & Dorey, P. (2023). Implementing partnerships in energy supply chain cybersecurity resilience. *Energies, 16*(4), 1868. https://doi.org/10.3390/en16041868
45. White House. (2024). *National security memorandum on critical infrastructure security and resilience* (NSM-22). https://www.presidency.ucsb.edu/documents/national-security-memorandum-critical-infrastructure-security-and-resilience