© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723364

A Threat-Driven Cyber Resilience Framework for Saudi Government Digital Services: Integrating Zero Trust, Security Operations and Adaptive Intelligence under Vision 2030

ILYAS SIDDIQUI MOHAMMAD
ORCiD: 0009-0009-5904-7181

Abstract- ***Saudi Arabia's rapid expansion of digital government has made cyber resilience a matter of public-service continuity rather than a purely technical security concern. Government platforms now depend on cloud services, shared data environments, mobile access, Internet of Things (IoT) devices, artificial intelligence, and increasingly interconnected critical systems. These developments improve the reach and efficiency of public services, but they also create dependencies that can amplify the effect of a cyber-incident. This review examines how a threat-driven cyber resilience approach combining integrated security architecture, cyber-threat intelligence (CTI), zero-trust principles, and adaptive security operations can enhance the continuity and protection of Saudi government digital services within the wider objectives of Vision 2030. A structured integrative review of 30 peer-reviewed studies, international cybersecurity frameworks, and Saudi regulatory publications issued between 2020 and 2025 was used to examine the relationship between governance, zero-trust access, security architecture, threat intelligence, security operations, and recovery. The evidence indicates that compliance controls are necessary but insufficient when identity, network, cloud, endpoint, data, and operational-technology protections operate as separate functions. Resilience improves when those controls are connected through common telemetry, context-aware access decisions, intelligence-led detection, governed automation, tested recovery, and post-incident learning. Saudi Arabia's National Cybersecurity Strategy and National Cybersecurity Authority (NCA) control families provide the national governance foundation, while NIST and CISA frameworks offer useful architectural and maturity guidance. Based on the synthesis, the paper proposes the Saudi Adaptive Cyber Resilience Architecture (SACRA), a threat-driven framework that connects mission assurance, zero-trust identity, protected infrastructure, intelligence-led security operations, adaptive response, recovery, and continuous evolution. The model is intended to support reliable public services, strengthen institutional readiness, and preserve confidence in the Kingdom's long-term digital transformation.***

Keywords: cyber resilience; Saudi Vision 2030; digital government; integrated security architecture; cyber-threat intelligence; zero trust; NCA; security operations.

I. INTRODUCTION

Digital transformation is a central feature of Saudi Arabia's public-sector modernization under Vision 2030. Government services are increasingly delivered through national platforms, cloud environments, mobile applications, shared data services, smart infrastructure, and interconnected systems. The benefits are substantial: services can be delivered at greater scale, data can move more quickly between authorized parties, and decision-making can be supported by digital information. At the same time, this degree of connectivity changes the nature of cyber risk. An incident affecting identity services, an application programming interface, a cloud configuration, a supplier, or an operational system may no longer remain confined to one technical component. It can disrupt several services at once and, in a government setting, may directly affect citizens, businesses, and essential operations.

Saudi cybersecurity policy already treats security as part of national development rather than as a separate technical activity. The National Cybersecurity Strategy describes the desired national cyberspace as secure, resilient, and trusted, and links cybersecurity to economic growth and prosperity (NCA, 2020a). Its emphasis on adaptive risk management, ecosystem assurance, dynamic defence, collaboration, and capability development is reinforced by later NCA

control sets for cloud services, data, operational technology, and essential cybersecurity requirements (NCA, 2020b; NCA, 2022a; NCA, 2022b; NCA, 2024a; NCA, 2024b). These instruments establish a strong governance baseline. However, a compliant organization may still experience serious service disruption if controls are bypassed, if a third party fails, or if recovery arrangements have not been tested against the dependencies of a critical service.

This distinction is important because cybersecurity and cyber resilience are related but not identical. Preventive security seeks to reduce the likelihood and impact of compromise. Resilience asks a broader operational question: can an organization continue or restore its most important functions when prevention is not fully successful? Reviews of cyber-resilience frameworks consistently place preparation, response, recovery, adaptation, and assessment alongside conventional risk reduction (Sepulveda Estay et al., 2020; Alhidaifi et al., 2024). For government digital infrastructure, the practical implication is that protection priorities should be derived from the public services that must remain available and from the systems, identities, data, suppliers, and recovery mechanisms on which those services depend.

The move away from a clearly bounded network perimeter makes this service-oriented view more urgent. Government users now connect through remote channels, cloud-hosted workloads, third-party platforms, mobile devices, APIs, and shared services. Under these conditions, physical or network location is a weak basis for trust. NIST's zero-trust architecture therefore shifts attention toward repeated verification of users, devices, workloads, and resources, with access decisions tied to policy and context rather than to presumed internal trust (Rose et al., 2020). CISA extends this approach through a maturity model covering identity, devices, networks, applications and workloads, and data, supported by visibility, analytics, automation, orchestration, and governance (CISA, 2023). For Saudi government entities, these principles are relevant because they provide a way to apply consistent trust decisions across mixed on-premise, cloud, mobile, and shared-service environments.

Architecture alone, however, cannot remain responsive to a changing threat environment. CTI gives technical observations meaning by relating indicators, vulnerabilities, adversary behaviour, infrastructure, and campaigns to specific risks and decisions. The literature suggests that intelligence becomes useful when it changes priorities: for example, when it informs vulnerability remediation, detection engineering, threat hunting, incident response, or strategic risk decisions (Cascavilla et al., 2021; Saeed et al., 2023; Ainslie et al., 2023). When CTI is connected to security information and event management, endpoint and identity telemetry, cloud monitoring, and orchestration platforms, an organization can adjust its defences as new evidence emerges instead of relying only on static control settings.

Against this background, the review asks how integrated security architecture and CTI can improve the cyber resilience of Saudi government digital infrastructure under Vision 2030. Four objectives guide the study. First, it synthesizes recent evidence on resilience-oriented security architecture. Second, it examines zero trust, CTI, automation, cloud security, critical-infrastructure protection, and emerging attack surfaces as connected rather than separate topics. Third, it considers how these themes relate to the Saudi cybersecurity governance framework. Finally, it develops an integrated implementation model for government digital services. The paper does not attempt to estimate national breach rates or technology-adoption percentages; the available evidence does not support such claims. Its contribution is instead a conceptually grounded synthesis focused on continuity, coordinated defence, and measurable recovery.

The paper makes four related contributions: (1) it synthesizes cyber-resilience, zero-trust, CTI, automation, cloud, IoT, 5G, OT, and supply-chain evidence into one service-oriented view; (2) it interprets international frameworks as implementation aids for Saudi national cybersecurity requirements; (3) it proposes a six-layer architecture linking governance and trust controls to security operations, response, recovery, and learning; and (4) it translates the synthesis into implementation priorities and measurable resilience outcomes for government digital services.

II. LITERATURE REVIEW

2.1 Cyber resilience as a design objective

Cyber resilience has developed from a narrow continuity concern into an enterprise design objective. Sepulveda Estay et al. (2020) show that existing assessment frameworks differ in structure, yet they repeatedly extend beyond prevention to include response, recovery, adaptation, and evaluation. Alhidaifi et al. (2024) reach a similar conclusion in their broader survey of cyber resilience. Taken together, these studies suggest that an organization cannot judge resilience solely by the number of preventive controls it has deployed. It must also understand how quickly it can absorb disruption, restore priority functions, and learn from the event. This is especially important for government services, where even a technically contained incident can become significant if it interrupts identity, payment, licensing, health, transport, or other public-facing functions.

The NIST Cybersecurity Framework (CSF) 2.0 reinforces this wider view by adding Govern as an explicit function alongside Identify, Protect, Detect, Respond, and Recover (Pascoe et al., 2024). Governance matters because resilience decisions depend on organizational context, risk appetite, accountability, policy, oversight, and supply-chain relationships. NIST SP 800-53 Rev. 5 provides a complementary control perspective by showing how security and privacy controls can be selected and tailored to organizational and system objectives (Ross and Pillitteri, 2020). In the Saudi context, these international frameworks are best treated as implementation aids rather than substitutes for NCA requirements. They can help an entity translate national controls into architecture decisions, control traceability, operational metrics, and recovery responsibilities.

Research on critical infrastructure also points toward integration. Malatji et al. (2022) argue that resilience depends on coordinated cybersecurity capabilities across increasingly connected environments, while Jiang et al. (2024) show how enterprise-architecture modelling can reveal relationships between business functions, information assets, applications, and technical infrastructure. That visibility is particularly valuable when a government service crosses organizational boundaries or relies on shared national platforms. A service cannot be prioritized effectively during an incident if its owners do not know which identities, networks, databases, suppliers, cloud components, or industrial systems are required to keep it operating. Architecture modelling therefore becomes part of resilience planning, not simply a documentation exercise.

2.2 Integrated security architecture and zero trust

An integrated security architecture is more than a collection of security products. It is a coordinated arrangement in which identity governance, device assurance, segmentation, application protection, data security, cloud controls, telemetry, incident response, and recovery are designed around common policies and service priorities. Zero trust provides a useful organizing principle because it removes the assumption that a request is safe merely because it originates from an internal network. Instead, access is evaluated using identity, device condition, context, resource sensitivity, and policy, and is limited to what is necessary for the task (Rose et al., 2020). The value of zero trust therefore lies less in a particular technology than in the discipline it imposes on trust decisions.

The literature also cautions against treating zero trust as a simple replacement project. He et al. (2022) identify authentication, access control, and trust assessment as important technical elements, but they also note the difficulty of maintaining reliable trust decisions across heterogeneous environments. Adahman et al. (2022) draw attention to migration cost and implementation complexity, while Kang et al. (2023) discuss the additional challenges created by cloud services and IoT environments. These concerns are directly relevant to large government estates, where legacy applications may coexist with modern cloud workloads and diverse connected devices. A phased migration, beginning with privileged identities and critical services, is therefore more consistent with the evidence than an abrupt enterprise-wide replacement of existing controls.

Cloud adoption introduces a related problem: responsibility is shared, but accountability for public-service continuity remains with the organization

delivering the service. Saudi Arabia's Cloud Cybersecurity Controls define requirements for both cloud service providers and cloud service tenants and therefore provide an important national baseline (NCA, 2020b; NCA, 2024b). Resilience requires those requirements to be integrated into day-to-day operations. Cloud security posture, privileged activity, key management, configuration changes, logging, and recovery arrangements should be visible to the teams responsible for identity, monitoring, incident response, and continuity. Without that integration, an entity may satisfy individual control requirements while still lacking an operational view of how a cloud failure or compromise would affect a critical government service.

Data protection follows the same logic. The NCA Data Cybersecurity Controls address the data lifecycle from creation and use through transmission, storage, archival, and disposal (NCA, 2022a), while SDAIA standards add governance expectations for classification, protection, accountability, and responsible management (SDAIA, 2021). The architectural challenge is to make classification consequential. A sensitive dataset should trigger appropriate access restrictions, encryption, monitoring, retention rules, backup requirements, and recovery priorities wherever it is processed. Treating classification as a label that is disconnected from technical controls weakens both security and resilience because the organization cannot consistently protect or restore information according to its operational importance.

2.3 Threat intelligence and security operations

CTI is valuable because it reduces uncertainty around cyber decisions. Cascavilla et al. (2021) show that useful cybercrime intelligence may draw on a wide range of sources, including information from the surface, deep, and dark web, but collection alone does not create operational value. The difficult step is turning observations into context that can guide action. Saeed et al. (2023) similarly identify CTI as an important contributor to organizational cyber resilience while noting persistent problems in information sharing, standardization, interoperability, and practical use. Ainslie et al. (2023) place particular emphasis on decision-making and the intelligence cycle. Read together, these studies suggest that the quality of CTI should be judged by the decisions it improves, not by the volume of indicators an organization receives.

For a government security operation, that means intelligence requirements should begin with mission questions. Analysts may need to know which actors or campaigns are targeting government identity systems, internet-facing applications, cloud tenants, key suppliers, or operational systems; which vulnerabilities are being exploited in relevant sectors; and which tactics are most likely to disrupt priority services. Those questions should shape collection and analysis. Internal telemetry, trusted partners, open and commercial sources, vulnerability information, incident reports, and national channels can then be normalized, enriched, assessed, and disseminated according to the needs of different audiences. A SOC may need observables and detection logic, a vulnerability team may need exploitation priorities, an architect may need likely attack paths, and an executive may need a clear statement of service risk and response options.

Automation can shorten the time between intelligence and defensive action, but the evidence does not support indiscriminate automation. Kinyua and Awuah (2021) describe SOAR as a way to coordinate security tasks and reduce repetitive analyst work, with growing opportunities for AI and machine learning. Dina and Manivannan (2021) show the potential of machine-learning-based intrusion detection to identify abnormal activity beyond known signatures, while Kaur et al. (2023) review how AI can contribute across several NIST cybersecurity functions. Salem et al. (2024) likewise report significant interest in AI-driven detection. Across these studies, however, performance remains dependent on data quality, suitable features, infrastructure, evaluation, and the management of false positives. Automation therefore improves speed only when it is supported by reliable inputs and clear governance.

A practical SOC model should distinguish between repeatable low-consequence actions and decisions that could disrupt an important service. Enrichment, indicator matching, case creation, evidence collection, and some temporary containment steps can often be

automated when confidence thresholds and rollback procedures are defined. Actions such as disabling a privileged national-service account, isolating a critical workload, or changing an OT process require a different level of authority because an incorrect response may itself create an outage. Human approval is therefore not a failure of automation; in high-impact situations it is part of the control design. The goal is to remove avoidable delay without transferring consequential decisions to systems that lack the operational context to judge their wider effect.

2.4 Expanding attack surfaces: IoT, 5G, software supply chains and OT

Saudi digital infrastructure increasingly combines conventional information systems with technologies that influence physical environments and public services. IoT is a clear example. Lone et al. (2023) identify recurring challenges associated with device heterogeneity, constrained computing resources, weak interfaces, insecure communications, and large-scale data collection. These weaknesses become more consequential when connected devices support transport, utilities, buildings, healthcare, public safety, or smart-city services. Resilience therefore requires more than network connectivity controls. Device identity, secure onboarding, firmware integrity, segmentation, telemetry, update mechanisms, and end-of-life management need to be considered across the device lifecycle.

5G creates a different but related set of dependencies. Its capacity and low-latency characteristics enable new digital services, yet the 5G core relies heavily on software-defined functions, virtualization, interfaces, and service-based communications. Tang et al. (2022) identify security concerns across authentication, network functions, slicing, interfaces, and the core architecture. For government consumers of 5G-enabled services, the implication is that connectivity should be treated as one component of a broader trust chain. A secure transport service does not remove the need to verify identities, protect workloads and APIs, monitor dependencies, or plan for failures in the services that sit above the network layer.

Operational technology raises the stakes further because a cyber incident can affect safety, availability, and physical processes as well as information. The NCA Operational Technology Cybersecurity Controls define minimum protection requirements for industrial control environments and explicitly place them within the national Vision 2030 context (NCA, 2022b). An integrated architecture should preserve the separation required between enterprise IT and OT while still enabling carefully controlled visibility and coordination. Secure remote access, identity governance, vulnerability management, monitored interfaces, incident escalation, backup arrangements, and recovery procedures must be designed around the operational constraints of the environment rather than copied directly from conventional IT practice.

Software supply chains create another path by which an external weakness can become an internal government risk. Reichert and Obelheiro (2024) describe exposure across development tools, third-party components, build processes, distribution, and external dependencies. A compromised package, update service, managed provider, or identity platform may enter through a trusted relationship and bypass controls that focus mainly on perimeter traffic. For that reason, supplier assurance should include visibility of software components, protected build and release processes, vulnerability management, signed artifacts where appropriate, incident-notification obligations, and workable recovery alternatives. These measures are especially important when a supplier holds privileged access or supports a service that cannot tolerate prolonged interruption.

2.5 Saudi governance context and research gap

The Saudi governance framework provides a strong policy base for this integrated view. The National Cybersecurity Strategy links protection to national resilience and prosperity (NCA, 2020a), while the Essential Cybersecurity Controls and specialized control families define expectations for essential cybersecurity, cloud services, data, and operational technology (NCA, 2022a; NCA, 2022b; NCA, 2024a; NCA, 2024b). The NCA's 2024 economic-indicators report adds another dimension by showing cybersecurity as a growing sector of employment and investment rather than only a compliance responsibility (NCA, 2024c). The challenge is therefore less about the absence of control requirements and more about how those requirements

are connected to operational architecture, threat information, and recovery decisions.

Research on Saudi digital government also highlights the importance of citizen experience and trust. Saeed (2025) reports that perceptions of usable security and privacy influence how people view electronic public services. This matters for resilience because service continuity is not only a technical measure. A service that is technically secure but difficult to use may encourage insecure workarounds, while poor communication about privacy or recovery can reduce confidence even after systems are restored. Security architecture therefore has to support both protection and a workable user experience, particularly for high-volume public services.

The existing literature provides valuable insights into individual cybersecurity capabilities, including cloud security, zero-trust architecture, threat intelligence, artificial intelligence-based detection, operational technology protection, and compliance frameworks. However, most studies examine these capabilities independently rather than explaining how they can operate together as an adaptive resilience system for government digital services. Limited research has addressed how threat intelligence can guide security priorities, enable faster operational decisions, support coordinated response, and improve recovery capability within a Saudi government context. This study addresses this gap by developing a threat-driven cyber resilience framework that integrates security architecture, intelligence operations, adaptive defence mechanisms, and continuous improvement principles aligned with Vision 2030 digital transformation objectives. Saudi regulations, meanwhile, establish the national control environment. What is less developed is an explanation of how these elements should operate as one resilience system for government digital services. This review addresses that gap by bringing governance, trust, architecture, intelligence, operations, response, recovery, and learning into a single model tailored to the Saudi context.

III. METHODOLOGY

This study uses a structured threat-oriented integrative review methodology. Unlike conventional reviews that examine individual cybersecurity technologies separately, this methodology focuses on identifying how different security capabilities interact as an adaptive operational system. The synthesis therefore evaluates relationships between threat intelligence, security operations, zero-trust implementation, incident response, recovery planning, and continuous resilience improvement. The method was selected because the research question spans several forms of evidence: technical security architecture, CTI, resilience research, national regulation, and digital-government governance. A conventional meta-analysis would not be appropriate for such a mixed evidence base because the included studies do not report a common quantitative outcome. The integrative approach instead combines a transparent search and selection process with thematic synthesis so that peer-reviewed research can be examined alongside authoritative standards and Saudi regulatory publications.

Sources were drawn from peer-reviewed literature associated with IEEE, ACM, Elsevier, Springer, Wiley, Emerald, and MDPI, together with official publications from the NCA, SDAIA, NIST, CISA, and other government bodies represented in the final evidence set. Searches combined terms relating to cyber resilience, digital government, integrated security architecture, zero trust, threat intelligence, SOC, SOAR, cloud security, critical infrastructure, IoT security, software supply chains, Saudi Arabia, NCA, and Vision 2030. The purpose of using several combinations was to capture evidence relevant to both the technical architecture of resilience and the governance context in which that architecture would operate.

A source was included when it made a clear contribution to at least one of four areas: resilience or architecture principles; evidence concerning CTI, detection, automation, or zero trust; emerging infrastructure risks relevant to government; or authoritative Saudi and international cybersecurity requirements. Sources outside the 2020-2025 period were excluded, as were duplicate versions, promotional material, and publications without a direct connection to cyber resilience. After applying these criteria, 30 sources remained in the final evidence set. The set intentionally combines scholarly work with official frameworks because the paper seeks to connect research findings with the control

environment faced by Saudi government organizations.

The selected material was analyzed in five stages. First, each source was coded according to its main contribution to governance, architecture and zero trust, CTI and security operations, infrastructure risk, or resilience. Second, the evidence was mapped against the functions of governing, identifying, protecting, detecting, responding, recovering, and adapting. Third, recurring implementation mechanisms were identified, including asset visibility, least privilege, segmentation, centralized telemetry, threat-informed detection, automation, backup integrity, supplier assurance, and post-incident learning. Fourth, these mechanisms were compared with Saudi national controls to identify where international evidence provided useful implementation logic for local requirements. Finally, the recurring themes were synthesized into the six-layer cyber-resilience architecture proposed later in the paper.

The review is conceptual rather than statistical, and its limitations follow from that choice. The 30 sources are not presented as an exhaustive account of every publication in cybersecurity, and the diversity of the material prevents a meaningful pooled-effect analysis. Instead, credibility is supported through triangulation. Major findings are based, where possible, on more than one type of evidence: peer-reviewed research is considered alongside recognized international frameworks and Saudi regulatory publications. This approach allows the analysis to distinguish between an academic argument, an architectural practice, and a formal control expectation while still examining how the three can support a common resilience objective.

Table 1. Evidence synthesis and architectural implications

Theme	Evidence synthesis (2020–2025)	Saudi government relevance	Architectural implication
Cyber-resilience governance	Governance connects cyber risk to mission, recovery and supply-chain decisions.	Supports NCA strategy/ECC implementation around critical public services.	Service criticality, accountable owners, recovery objectives and control traceability.
Zero trust and identity	Continuous verification reduces implicit trust across hybrid environments.	Useful for shared platforms, cloud access, privileged administration and remote services.	Strong identity, PAM, device posture, least privilege and contextual authorization.
Threat intelligence	CTI creates value when it answers decision requirements and feeds operations.	Enables threat-informed prioritization across ministries and shared national dependencies.	Priority intelligence requirements, enrichment, detection engineering and feedback loops.
Cloud and data assurance	Shared responsibility and lifecycle controls must be operationally integrated.	Aligns cloud tenants/providers with NCA CCC and data protection expectations.	Central identity, posture assurance, key management, classification-led controls and logging.
IoT, 5G and OT	Connected technologies expand attack paths into physical and mission-critical environments.	Relevant to smart government, infrastructure, transport and industrial services.	Segmentation, device identity, monitored remote access, lifecycle security and recovery planning.
Supply-chain resilience	Third-party software and privileged services can become internal attack paths.	Government platforms often depend on vendors, MSPs, cloud and telecom providers.	Tiered supplier assurance, contractual notification, build integrity and alternative recovery options.
Automation and AI	Automation can accelerate enrichment and response but requires governance.	Reduces SOC burden without delegating high-consequence decisions blindly.	Risk-tiered playbooks, human approval thresholds, rollback,

			audit trails and model monitoring.

3.1 Search transparency and PRISMA-informed reporting.

The review is a structured integrative literature review with PRISMA 2020-informed reporting rather than a fully reproducible systematic review. Searches were described for Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink and publisher databases, using combinations of cyber resilience, digital government, integrated security architecture, zero trust, cyber-threat intelligence, SOC, SOAR, cloud security, critical infrastructure, IoT, 5G, software supply chain, Saudi Arabia, NCA and Vision 2030. The substantive evidence window was 2020-2025. Original database exports, exact retrieval counts, deduplication logs and exclusion logs were not retained in the source record; those values are therefore reported as NR rather than retrospectively invented. The final evidence set and bibliography remain auditable, and the absence of intermediate counts is treated as a methodological limitation (Page et al., 2021).

3.2 Eligibility, appraisal and synthesis

Peer-reviewed studies were included when they directly informed resilience architecture, threat intelligence, detection, zero trust, cloud or OT security, response, recovery, or Saudi digital-government governance. Authoritative Saudi and international standards were included as requirement or guidance sources, not as empirical proof of effectiveness. Quality appraisal considered methodological transparency, relevance to the review questions, deployment realism, treatment of false positives or operational consequence, and clarity of limitations. Evidence was coded into governance, trust, protected infrastructure, CTI/security operations, response/recovery, and learning themes. Source status is distinguished as peer-reviewed evidence, Saudi regulatory requirement, international guidance, or author synthesis so that normative controls are not confused with validated outcomes.

3.3 Saudi applicability and validation status.

The six-layer architecture is proposed and validation-ready; it is not presented as empirically validated across Saudi government entities. Saudi-specific applicability is illustrated through service archetypes rather than claims about unobserved agency configurations: national identity and justice transactions, health-service access, data-governance platforms, cloud-hosted public services, and inter-agency information exchange. Relevant governance actors and instruments include the Digital Government Authority, NCA, SDAIA/NDMO, and the Personal Data Protection Law. A future validation programme should combine expert review by Saudi cybersecurity professionals with a controlled case study or architecture simulation. Validation evidence should include dependency maps, detection and containment timelines, recovery-test artifacts, expert ratings, identified failure modes, and documented changes to the framework.

Table 2. PRISMA-informed search and reporting record

Element	Reported approach	Audit status
Databases	Scopus; Web of Science; IEEE Xplore; ScienceDirect; SpringerLink; publisher databases	Specified
Search terms	Resilience + architecture + CTI + zero trust + SOC/SOAR + Saudi/NCA/Vision 2030 combinations	Specified concept blocks
Evidence window	2020-2025	Specified
Search dates / retrieved records	Original dates and database counts	NR - source logs not retained

Duplicates / screening / exclusions	No preserved database export or exclusion log	NR - not invented
Final corpus	Final cited evidence and authoritative requirements	Auditable from references
Quality appraisal	Relevance, methodological transparency, realism, limitations, operational consequence	Applied qualitatively

IV. RESULTS AND DISCUSSION

4.1 Finding 1: resilience depends on integration across control domains

The clearest finding across the reviewed material is that individual controls can improve local security without necessarily creating resilience at service level. A government digital service is rarely supported by one system. It depends on identities, applications, APIs, cloud resources, databases, endpoints, networks, suppliers, and operational processes that interact as a chain. A weakness in one of those dependencies can affect the whole service even when the remaining controls perform as intended. Integrated architecture addresses this problem by defining common trust decisions, telemetry expectations, asset relationships, response procedures, and recovery priorities. Enterprise-architecture modelling is useful here because it links technical components to the business or public-service functions they support (Jiang et al., 2024).

For a ministry or government agency, the starting point should therefore be the critical service rather than the security product. The organization needs to know which data is authoritative, which users and privileged roles are involved, which applications and infrastructure are required, which external services are dependencies, where logs are produced, who owns recovery decisions, and what level of interruption is acceptable. This mapping creates a practical basis for prioritization. It also makes NCA requirements easier to interpret operationally because controls can be related to the importance of the service they protect rather than managed as isolated checklist items.

Zero trust supports this integration by applying a consistent approach to access across those dependencies. Its contribution is architectural discipline: implicit trust is reduced, permissions are narrowed, and authentication and authorization decisions are informed by identity, device, context, and resource sensitivity (Rose et al., 2020; He et al., 2022). CISA's maturity model provides a practical route for progressing from partial controls toward more consistent enforcement. The implementation concerns identified by Adahman et al. (2022) and Kang et al. (2023) indicate that adoption should be phased around risk, legacy constraints, cloud workloads, and IoT diversity. In a Saudi government environment, privileged identities and high-value services are a logical first focus before extending continuous controls to devices, workloads, networks, and data.

4.2 Finding 2: CTI is the adaptive layer of integrated architecture

CTI becomes an adaptive layer when it connects technical evidence to specific decisions. An IP address, domain, file hash, vulnerability, or malware signature has limited value on its own. Its significance changes when analysts can relate it to an adversary, campaign, tactic, target sector, exploitation pattern, or service dependency (Cascavilla et al., 2021; Ainslie et al., 2023). This distinction matters in government operations because defenders rarely have unlimited time or resources. They need to determine which alerts, vulnerabilities, identities, and external dependencies are most likely to affect services that matter to the public.

A mature CTI process should therefore begin with prioritized intelligence requirements. These requirements may concern threats to identity infrastructure, cloud tenants, public websites, suppliers, or operational systems. Collection can then draw on internal telemetry, trusted partners, vulnerability information, incident reports, national

channels, and appropriate open or commercial sources. The output should be adapted to the audience rather than distributed in one generic format. SOC analysts need detection logic and observables; vulnerability teams need evidence of exploitation and likely impact; architects need adversary techniques and attack paths; and senior decision-makers need a concise explanation of service risk, urgency, and available options.

The resilience benefit appears when this intelligence changes control behaviour. Evidence of credential theft may justify stronger authentication checks or closer session monitoring. Confirmed exploitation of an internet-facing product may alter patching priorities or trigger a temporary compensating control. A campaign affecting a supplier may justify tighter monitoring of third-party identities. Intelligence about destructive malware may lead continuity teams to verify backup integrity sooner than planned. In each case, CTI closes the gap between observation and adaptation. It becomes part of protection, detection, response, and recovery rather than a reporting function that sits beside them.

4.3 Finding 3: automation should accelerate governed response, not replace judgment

The volume of telemetry generated by endpoints, identities, cloud platforms, networks, applications, and IoT devices can exceed what a manual SOC can review consistently. SOAR and AI-supported detection offer a way to reduce repetitive work through enrichment, correlation, prioritization, and repeatable response actions (Kinyua and Awuah, 2021; Dina and Manivannan, 2021; Kaur et al., 2023; Salem et al., 2024). The evidence supports their use as force multipliers, but it does not suggest that automation should be allowed to make every operational decision. The value of automation depends on dependable data, appropriate confidence thresholds, and clear ownership of consequences.

Low-risk tasks are the strongest candidates for automatic execution. These may include collecting endpoint artifacts, enriching an alert with asset and identity context, checking indicators against intelligence sources, opening a case, or applying a temporary block to a known malicious domain when confidence is high. Medium-impact actions, such as isolating a workstation or revoking a suspicious token, may require analyst approval depending on the affected user and service. Actions that could interrupt a critical workload, privileged identity, or OT process should remain under designated authority. The distinction is important because response speed is useful only when the response itself does not create greater disruption than the threat.

Governed automation also requires traceability. A playbook should record what triggered an action, which evidence supported it, which policy allowed it, who approved it where approval was required, and how the action could be reversed. These records are especially important in public institutions, where accountability and service impact matter alongside technical efficiency. AI-assisted detection needs similar discipline. Models should be evaluated for false positives, drift, performance differences between environments, and possible adversarial manipulation. Continuous review is therefore part of safe automation rather than an optional activity after deployment.

4.4 Finding 4: cloud, data, IoT, 5G and OT require one risk language

Saudi control frameworks address cloud services, data, essential systems, and operational technology through specialized requirements. The operational difficulty is that organizations may implement these requirements through separate teams with different terminology and risk priorities. A common service-oriented risk language can reduce that fragmentation. Risk decisions can be framed around mission impact, asset criticality, exposure, trust relationships, threat relevance, control strength, and the ability to recover. Using those dimensions makes it possible to compare apparently different issues, such as a cloud misconfiguration, an exposed API, a compromised identity, an IoT gateway, or an OT remote-access path, according to their potential effect on the same public service.

The reviewed evidence supports this cross-domain treatment. Cloud controls need to connect tenant responsibility with central identity, key management, configuration assurance, logging, and incident response (NCA, 2020b; NCA, 2024b). Data classification should influence access, encryption, monitoring, retention, and recovery (NCA, 2022a;

SDAIA, 2021). IoT environments require device identity, segmentation, update mechanisms, and lifecycle visibility (Lone et al., 2023). 5G-enabled services need assurance above the transport layer because virtualized functions and service-based communications create their own dependencies (Tang et al., 2022). OT environments, meanwhile, require strict change control, monitored remote access, segmentation, and recovery arrangements that respect safety and availability constraints (NCA, 2022b).

The practical implication is that security architecture should be part of digital-service design rather than a review performed after deployment. A new service should be able to show how users and workloads are authenticated, how sensitive information is classified, which telemetry is generated, which external dependencies are monitored, how an incident would be contained, and how the service would be restored. Asking these questions early exposes resilience gaps while design choices can still be changed. It also creates a traceable connection between national control requirements and the way a service actually operates.

4.5 Finding 5: supply-chain and third-party resilience must be treated as internal risk

Software supply-chain exposure should be treated as an internal resilience concern when a supplier is embedded in a critical service. Reichert and Obelheiro (2024) show that risk can enter through development infrastructure, third-party packages, build processes, distribution, and external dependencies. A supplier with privileged access, a managed service provider, a software library, or an update mechanism can become part of the organization's effective attack surface. Traditional questionnaires may provide useful governance information, but they do not by themselves show whether the technical dependency is being monitored or whether the organization can continue operating if the supplier becomes unavailable or compromised.

Supplier assurance should therefore be proportionate to service criticality and technical dependency. High-impact suppliers should be able to demonstrate secure development practices, vulnerability management, incident notification, privileged-access control, appropriate logging, backup and recovery capability, and supply-chain protection. Contracts can define notification and cooperation requirements, but architecture must also limit unnecessary third-party privilege and monitor the identities and connections that suppliers use. Where feasible, important services should retain a practical exit, fallback, or recovery option so that a supplier incident does not become an unavoidable government-service outage.

4.6 Finding 6: governance and workforce determine whether architecture functions in practice

The NIST CSF 2.0 places governance at the centre of cybersecurity risk management, and the Saudi National Cybersecurity Strategy similarly emphasizes organization, policy, collaboration, and ecosystem development (Pascoe et al., 2024; NCA, 2020a). The NCA's economic-indicators report further presents cybersecurity as a growing national capability supported by workforce and investment (NCA, 2024c). These sources point to a basic limitation of architecture: controls cannot operate coherently if responsibilities are unclear. Resilience therefore depends on governance arrangements that connect technical ownership with service accountability and executive decision-making.

Government entities need identifiable owners for critical services, cyber risk, identity, data, cloud services, suppliers, incident response, and recovery. Architecture standards should define the minimum expectations for telemetry, identity controls, logging, segmentation, and resilience so that teams do not design these elements independently. SOC and CTI functions should also have established working relationships with infrastructure, application, risk, legal, privacy, continuity, and executive teams. Exercises are especially valuable when they include both technical responders and service owners, because that is where decisions about containment, downtime, communication, and restoration can be tested against actual public-service priorities.

Usability is part of this governance problem as well. Saeed (2025) shows that usable security and privacy shape citizens' perceptions of Saudi digital public services. Controls that are technically strong but unnecessarily difficult can encourage users to seek workarounds, while unclear privacy practices may reduce confidence in otherwise reliable services.

Resilient design should therefore combine strong authentication and protection with understandable user journeys, clear communication, and recovery processes that still work under pressure. Public trust is affected not only by whether an incident occurs, but also by how well the service and the institution respond when one does.

4.7 Comparison with Existing Cyber Resilience Approaches

Several cybersecurity frameworks and resilience approaches have been developed to improve organisational protection against cyber threats. However, existing approaches generally address specific aspects of cybersecurity, such as governance, identity management, or cloud protection. This study proposes the Saudi Adaptive Cyber Resilience Architecture (SACRA) as an integrated, threat-driven framework that combines these capabilities into a coordinated model for government digital service resilience. Table 4 presents a comparison between established approaches and the proposed framework.

Table 4. Comparison of Existing Cyber Resilience Approaches with SACRA

Approach	Primary Focus	Limitation
NIST Cybersecurity Framework (CSF)	Provides cybersecurity governance through Identify, Protect, Detect, Respond and Recover functions	A general framework that requires adaptation for specific government digital service environments
Zero Trust Architecture	Focuses on identity verification, least privilege access and continuous trust evaluation	Mainly addresses access security and does not provide a complete resilience lifecycle including recovery and learning
Cloud Cyber Resilience Models	Focus on cloud availability, cloud governance, backup and disaster recovery	Primarily designed for cloud environments and may not address wider government infrastructure dependencies
Traditional Cybersecurity Compliance Models	Focus on regulatory controls and security requirements	Compliance achievement does not always guarantee operational resilience during cyber incidents
Saudi Adaptive Cyber Resilience Architecture (SACRA)	Threat-driven government digital service resilience integrating intelligence, zero trust, security operations, response and continuous improvement	Requires future validation through government case studies and operational testing

V. PROPOSED SAUDI ADAPTIVE CYBER RESILIENCE ARCHITECTURE (SACRA)

The synthesis supports the Saudi Adaptive Cyber Resilience Architecture (SACRA), a six-layer threat-driven model designed specifically for government digital service resilience. Unlike traditional security models that focus primarily on prevention and compliance, SACRA emphasizes continuous threat awareness, adaptive defence, and operational recovery. The first layer establishes mission assurance and governance by defining service criticality, regulatory alignment, risk ownership, data classification, and recovery objectives. The second layer focuses on zero-trust identity and trust management, including authentication, privileged-access management, device assurance, least privilege, and contextual authorization. The third layer protects digital infrastructure through segmentation, cloud security, application protection, endpoint controls, cryptographic protection, and IT/OT boundary management, where NCA requirements, service criticality, risk ownership, data classification, and recovery objectives are defined. The second layer is identity and trust, covering strong authentication,

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723364

privileged-access management, device posture, least privilege, and context-aware authorization. The third layer is protected digital infrastructure, including segmentation, cloud security, application and API protection, endpoint controls, secure configuration, cryptography, and appropriate IT/OT boundaries. The fourth layer is security operations and threat intelligence. Here, telemetry from identities, endpoints, networks, cloud services, applications, data platforms, and selected OT sources is normalized and enriched with adversary and vulnerability context so that detection and prioritization reflect the risks facing each service.

The fifth layer is coordinated response and recovery. It brings together incident management, SOAR playbooks, defined containment authority, backup integrity, disaster-recovery arrangements, alternative service paths, and crisis communication. The sixth layer is learning and adaptation. Incidents, exercises, threat intelligence, control assessments, supplier events, and service failures should produce changes to architecture, detections, procedures, and risk priorities. The value of the model lies in the connections between layers. Governance establishes what is important; trust and infrastructure controls protect it; security operations create visibility; intelligence changes priorities; response limits disruption; recovery restores service; and lessons from the event reshape the next cycle of decisions.

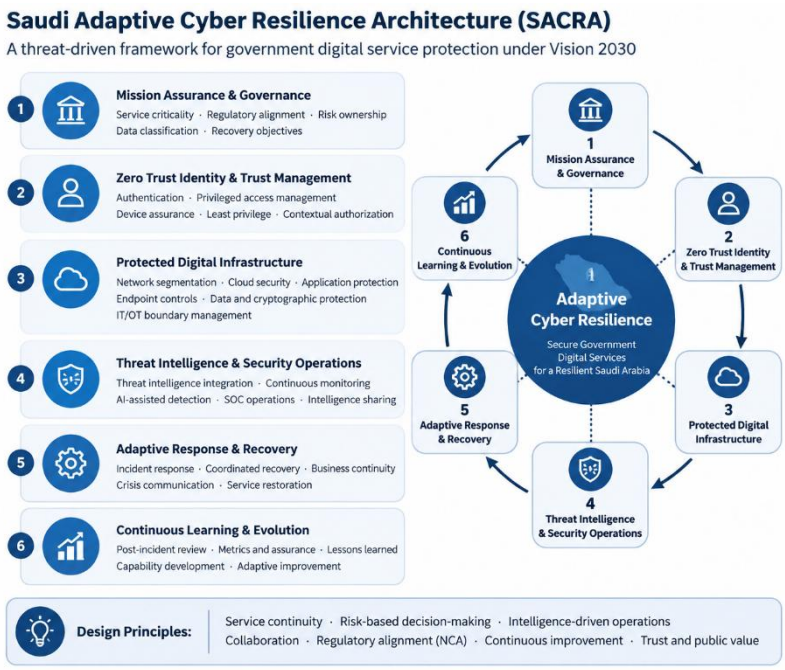

Figure 1. Saudi Adaptive Cyber Resilience Architecture (SACRA) for Threat-Driven Government Digital Service Protection.

The architecture can be assessed through measures that reflect service outcomes rather than control counts alone. Useful indicators include the proportion of critical services with documented dependency maps, the coverage of privileged identities under continuous control, telemetry coverage for critical assets, the time required to validate a high-confidence threat, containment time, restoration performance against agreed service objectives, successful backup recovery tests, unresolved high-risk supplier findings, and the closure of lessons identified during incidents and exercises. No single measure proves resilience, but together they show whether the organization can see its dependencies, act on relevant threats, contain disruption, and restore priority services in a controlled manner.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723364

VI. IMPLEMENTATION PRIORITIES AND IMPLICATIONS

Implementation should begin with the services whose disruption would have the greatest public or operational consequence. For each one, the entity should map the identities, applications, data, infrastructure, suppliers, and recovery dependencies that support delivery. Identity and privileged-access controls can then be strengthened around those services, because compromised credentials often provide a route between otherwise well-defended environments. The next priority is to integrate telemetry and define CTI requirements that are tied to specific service risks. Segmentation, cloud hardening, data controls, and API protection can then be prioritized using threat relevance and dependency information rather than being applied only by technology category.

Response and continuity planning should develop in parallel with these preventive controls. SOC, incident-response, and continuity teams should maintain joint playbooks for scenarios such as identity compromise, ransomware, cloud outage, supplier breach, destructive malware, data exfiltration, and OT intrusion. Recovery objectives, backup integrity, decision authority, communication responsibilities, and fallback arrangements should be tested rather than assumed. The final implementation priority is continuous improvement. Maturity measures, incident reviews, exercises, and new threat information should be used to identify recurring weaknesses and to update architecture, detections, supplier controls, and recovery arrangements. This creates a cycle in which resilience is progressively improved instead of treated as a one-time compliance project.

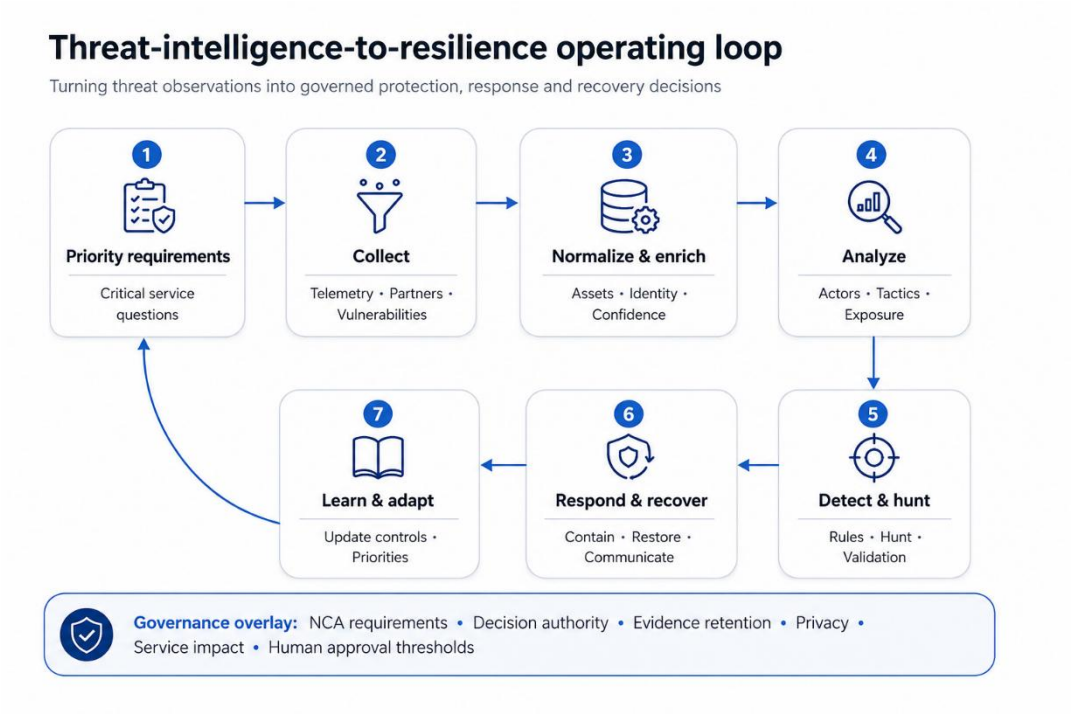

Figure 2. Threat-intelligence-to-resilience operating loop.

The threat-intelligence-to-resilience loop depends on information that can move between teams and, where appropriate, between organizations. Standardized telemetry fields, trusted exchange mechanisms, sector-specific threat profiles, reusable detection content, and coordinated exercises can help entities learn from incidents affecting their peers. Such collaboration is consistent with the whole-of-nation and collaborative-security principles of the Saudi strategy. Its practical value is speed: one organization's experience can improve another organization's detection priorities, defensive controls, or recovery readiness before the same threat produces a comparable disruption.

Table 3. Phased implementation roadmap and resilience metrics

Phase	Priority actions	Primary alignment	Example outcome metrics
1. Map critical services	Identify services, identities, applications, data, infrastructure, suppliers and recovery dependencies.	NCA strategy; ECC governance/resilience	% critical services with dependency maps; named service owners.
2. Strengthen trust	Prioritize privileged identities, MFA, device posture and least-privilege access.	ECC; NIST ZTA; CISA ZTMM	% privileged identities under PAM/continuous control; stale privilege reduction.
3. Integrate telemetry & CTI	Standardize logs; connect CTI requirements to services; enrich alerts with asset and identity context.	ECC defence; national collaborative-security goal	Telemetry coverage; mean time to validate high-confidence threats.
4. Harden cloud, data & segmentation	Apply cloud posture, classification-led controls, key management, API protection and segmentation.	CCC; DCC; OTCC	Critical misconfiguration closure; segmentation coverage; protected sensitive-data flows.
5. Govern response & recovery	Joint SOC/IR/continuity playbooks; backup integrity; alternative service paths; exercises.	ECC resilience; OTCC	Containment time; restoration time vs objectives; backup recovery success.
6. Learn and adapt	Close lessons from incidents/exercises; update architecture, detections, supplier controls and priorities.	Strategy adaptive-risk and dynamic-defense goals	% lessons closed on time; recurring-control failures; unresolved high-risk supplier findings.

VII. CONCLUSION

Saudi Arabia's digital-government ambitions depend on cybersecurity that protects systems and data while also preserving the continuity of public services. The evidence reviewed in this paper indicates that resilience is strongest when governance, zero trust, security architecture, CTI, security operations, automation, response, and recovery are treated as parts of one operating system. Perimeter controls and compliance requirements remain important, but they cannot address the full effect of interconnected identities, cloud platforms, APIs, IoT devices, suppliers, 5G-enabled services, and operational technology when these dependencies are managed separately.

The Saudi National Cybersecurity Strategy and NCA control families provide a clear national foundation for this approach. NIST and CISA frameworks add useful guidance on governance, architecture, zero trust, and maturity, while recent research provides evidence on CTI, AI-assisted detection, SOAR, enterprise architecture, critical-infrastructure resilience, and emerging attack surfaces. Across these sources, the recurring issue is not the absence of individual controls. It is the need to connect them. Critical-service dependencies must be visible, trust decisions must be contextual, telemetry must be usable across operational teams, intelligence must alter priorities, response authority must be governed, and recovery must be exercised against realistic service objectives.

The main contribution of this research is the development of a threat-driven resilience perspective that moves beyond isolated security controls and compliance-based protection. By connecting intelligence generation, operational decision-making, adaptive defence, and recovery capability, SACRA provides a structured approach for government entities seeking to improve resilience against evolving cyber threats.

The proposed six-layer architecture translates that synthesis into a practical model for Saudi government

entities pursuing Vision 2030 objectives. Its purpose is not to recommend another collection of security products. Instead, it provides a way to connect existing governance and technical capabilities around the public services that matter most. Future research should test the model across different government settings, examine whether the proposed maturity measures distinguish stronger from weaker resilience practices, and study how inter-agency intelligence exchange affects detection and recovery outcomes. Such empirical work would help move cyber resilience from an important strategic principle toward a capability that can be observed, tested, and improved over time. The methodology also makes the validation boundary explicit: the framework is a structured proposal rather than a claim of observed performance across Saudi government entities.

REFERENCES

[1] Z. Adahman, A. W. Malik, and Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," *Computers & Security*, vol. 122, Art. no. 102911, 2022, doi: 10.1016/j.cose.2022.102911. ScienceDirect

[2] S. Ainslie, D. Thompson, S. B. Maynard, and A. Ahmad, "Cyber-threat intelligence for security decision-making: A review and research agenda for practice," *Computers & Security*, vol. 132, Art. no. 103352, 2023, doi: 10.1016/j.cose.2023.103352. ScienceDirect

[3] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, "A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions," *ACM Computing Surveys*, vol. 56, no. 8, Art. no. 196, pp. 1–48, 2024, doi: 10.1145/3649218. ACM

[4] G. Cascavilla, D. A. Tamburri, and W.-J. Van Den Heuvel, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Computers & Security*, vol. 105, Art. no. 102258, 2021, doi: 10.1016/j.cose.2021.102258. Crossref

[5] Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model*, Version 2.0. Washington, DC, USA: CISA, 2023. CISA

[6] A. S. Dina and D. Manivannan, "Intrusion detection based on Machine Learning techniques in computer networks," *Internet of Things*, vol. 16, Art. no. 100462, 2021, doi: 10.1016/j.iot.2021.100462. Crossref

[7] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wireless Communications and Mobile Computing*, vol. 2022, Art. no. 6476274, 2022, doi: 10.1155/2022/6476274. Crossref

[8] Y. Jiang, M. A. Jeusfeld, M. Mosaad, and N. Oo, "Enterprise architecture modeling for cybersecurity analysis in critical infrastructures—A systematic literature review," *International Journal of Critical Infrastructure Protection*, vol. 46, Art. no. 100700, 2024, doi: 10.1016/j.ijcip.2024.100700. ScienceDirect

[9] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," *Entropy*, vol. 25, no. 12, Art. no. 1595, 2023, doi: 10.3390/e25121595. MDPI

[10] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, Art. no. 101804, 2023, doi: 10.1016/j.inffus.2023.101804. Crossref

[11] J. Kinyua and L. Awuah, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 527–545, 2021, doi: 10.32604/iasc.2021.016240. Tech Science Press

[12] A. N. Lone, S. Mustajab, and M. Alam, "A comprehensive study on cybersecurity challenges and opportunities in the IoT world," *Security and Privacy*, vol. 6, no. 6, Art. no. e318, 2023, doi: 10.1002/spy2.318. Wiley

[13] M. Malatji, A. L. Marnewick, and S. von Solms, "Cybersecurity capabilities for critical infrastructure resilience," *Information & Computer Security*, vol. 30, no. 2, pp. 255–279, 2022, doi: 10.1108/ICS-06-2021-0091. Emerald

[14] National Cybersecurity Authority, *National Cybersecurity Strategy*. Riyadh, Saudi Arabia: Kingdom of Saudi Arabia, 2020.

[15] National Cybersecurity Authority, *Cloud Cybersecurity Controls (CCC-1:2020)*. Riyadh,

Saudi Arabia: Kingdom of Saudi Arabia, 2020. NCA

[16] National Cybersecurity Authority, *Data Cybersecurity Controls (DCC-1:2022)*. Riyadh, Saudi Arabia: Kingdom of Saudi Arabia, 2022. NCA

[17] National Cybersecurity Authority, *Operational Technology Cybersecurity Controls (OTCC-1:2022)*. Riyadh, Saudi Arabia: Kingdom of Saudi Arabia, 2022. NCA

[18] National Cybersecurity Authority, *Essential Cybersecurity Controls (ECC 2-2024)*. Riyadh, Saudi Arabia: Kingdom of Saudi Arabia, 2024. NCA

[19] National Cybersecurity Authority, *Cloud Cybersecurity Controls (CCC-2:2024)*. Riyadh, Saudi Arabia: Kingdom of Saudi Arabia, 2024. NCA

[20] National Cybersecurity Authority, *Report on Key Economic Indicators in the Cybersecurity Sector of 2024*. Riyadh, Saudi Arabia: Kingdom of Saudi Arabia, 2024. NCA

[21] C. Pascoe, S. Quinn, and K. Scarfone, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29. NIST

[22] B. M. Reichert and R. R. Obelheiro, "Software supply chain security: a systematic literature review," *International Journal of Computers and Applications*, vol. 46, no. 10, pp. 853–867, 2024, doi: 10.1080/1206212X.2024.2390978. Taylor & Francis

[23] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207. NIST

[24] R. S. Ross and V. Y. Pillitteri, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Revision 5. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-53r5. NIST

[25] S. Saeed, "Digital Transformation in Governmental Public Service Provision and Usable Security Perception in Saudi Arabia," *Information*, vol. 16, no. 3, Art. no. 247, 2025, doi: 10.3390/info16030247. MDPI

[26] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," *Sensors*, vol. 23, no. 16, Art. no. 7273, 2023, doi: 10.3390/s23167273. MDPI

[27] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *Journal of Big Data*, vol. 11, Art. no. 105, 2024, doi: 10.1186/s40537-024-00957-y. Springer

[28] Saudi Data and Artificial Intelligence Authority, *Data Management and Personal Data Protection Standards*, Version 1.5. Riyadh, Saudi Arabia: National Data Management Office, 2021.

[29] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Computers & Security*, vol. 97, Art. no. 101996, 2020, doi: 10.1016/j.cose.2020.101996. ScienceDirect

[30] Q. Tang, O. Ermis, C. D. Nguyen, A. De Oliveira, and A. Hirtzig, "A Systematic Analysis of 5G Networks With a Focus on 5G Core Security," *IEEE Access*, vol. 10, pp. 18298–18319, 2022, doi: 10.1109/ACCESS.2022.3151000. IEEE