Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

REAL-TIME AI-DRIVEN CYBERSECURITY ANALYTICS DASHBOARDS FOR CRITICAL-INFRASTRUCTURE PROTECTION UNDER SAUDI VISION 2030: AN NCA- AND SDAIA-ALIGNED GOVERNANCE-TO-EXECUTION FRAMEWORK

Choudhry Bilal Mazhar Hussain[1]

[1]Arabian Agricultural Services Company (ARASCO), Riyadh, Kingdom of Saudi Arabia

Corresponding author: cbmr.bilal@gmail.com | ORCID: 0009-0005-7625-7296

Abstract

Saudi Arabia's Vision 2030 has accelerated the adoption of artificial intelligence, data governance, cloud platforms and digital public services, making cybersecurity a strategic condition for resilient transformation. This paper develops a PRISMA-informed design-science framework for real-time AI-driven cybersecurity analytics dashboards aligned with the National Cybersecurity Authority (NCA), the Saudi Data & AI Authority (SDAIA), the National Data Management Office (NDMO), the Personal Data Protection Law (PDPL), and Vision 2030 priorities. The study synthesizes academic literature, Saudi policy artefacts, regulatory guidance and selected industry threat reports to address an execution gap between strategic cyber-governance commitments and auditable, operational, real-time decision systems. The proposed framework contributes a dashboard typology, a five-layer reference architecture, a sectoral applicability matrix, an operational threat-to-control mapping, a KPI dictionary, a Responsible-AI implementation matrix and an indicative 180-day pilot pathway. The findings emphasize that dashboards do not independently create cyber-resilience; they may support resilience only when

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

telemetry coverage, model governance, human oversight, compliance evidence and response workflows are implemented and validated together. The NCA/SDAIA/NDMO/PDPL alignment is context-specific to Saudi Arabia, while the layered architecture and governance logic are transferable to other jurisdictions if localized to relevant legal and regulatory environments. The paper contributes to cybersecurity governance, AI assurance, SOC maturity, critical-infrastructure protection and digital analytics research by positioning real-time dashboards as governed socio-technical decision systems rather than isolated visualization artefacts.

Keywords: Artificial Intelligence; Cybersecurity Analytics; Cyber Resilience; Critical Infrastructure; Saudi Vision 2030

1. Introduction

Saudi Arabia's Vision 2030 has made data, artificial intelligence and digital government capability central to national transformation. SDAIA and the National Strategy for Data & AI position data and AI as strategic national enablers, while the NCA frames cybersecurity as a prerequisite for protecting national security, critical infrastructure and priority sectors [1–5]. In this environment, cybersecurity dashboards cannot be treated as simple operational screens. They increasingly operate as boundary objects between SOC operations, compliance evidence production, AI model governance and executive accountability.

The research gap addressed in this paper is an execution gap: the distance between policy frameworks and interoperable, audit-ready, real-time cyber-governance. The central research question is: how can real-time AI-driven cybersecurity analytics dashboards be designed as governed decision systems for Saudi critical-infrastructure

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

protection while preserving the distinction between security operations, compliance evidence, model governance, executive risk oversight and sectoral or national cyber-posture reporting?

The paper's contribution is conceptual and translational. It does not claim empirical detection of improvement or deployed system performance. Instead, it offers a design-science artefact set consisting of a conceptual model, a five-layer reference architecture, dashboard typology, control taxonomy, KPI dictionary, Responsible-AI matrix, and pilot pathway. This positioning responds to the need for clearer operationalization of cybersecurity governance under AI-enabled digital transformation.

The framework is intended for enterprise deployment first; sectoral aggregation second and national posture reporting only where lawful aggregation, anonymization and regulator-defined reporting rules exist. It is not proposed as a single national surveillance dashboard. At enterprise level, it supports SOC, CISO, GRC, and AI-governance decision-making. At national level, only standardized and non-identifying posture indicators should be shared.

2. Literature Review

The manuscript is positioned as a PRISMA-informed design-science framework paper. In design-science research, knowledge is created by developing artefacts that address human, organizational and technical problems [19,20]. This paper follows that logic by developing a governed dashboard architecture and associated decision instruments. The PRISMA-informed synthesis provides structured evidence for the artefact design, but it does not establish causal effectiveness.

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

Cyber-resilience is broader than threat prevention or alerting. It concerns the capacity to anticipate, withstand, recover from, and adapt to adverse cyber conditions [23,31,34]. This orientation is important for critical infrastructure because resilient performance depends not only on detection technology but also on governance accountability, tested response workflows, human decision rights, recovery capability and the ability to adapt after disruption. Information security and cyber-governance research similarly emphasizes that public-sector and enterprise cyber-risk management must connect policy, risk ownership, control evidence, and operational accountability [21,39].

Security Operations Centers and SIEM platforms provide the operational foundation for real-time detection and response. Prior SOC research highlights that SOC effectiveness depends on coordinated people, processes and technology rather than tooling alone [26,27]. SIEM literature shows a shift from monitoring and alerting toward compliance-aware, analytics-enabled and critical-infrastructure-relevant security monitoring [28,29]. Enterprise cybersecurity analytics literature further emphasizes the need to connect data integration, detection logic, analytics maturity, and organizational decision-making [30].

AI assurance and trustworthy AI research are directly relevant because AI-enabled cyber-analytics may produce false positives, false negatives, concept drift, adversarial vulnerabilities, and explainability challenges. Trustworthy AI frameworks therefore require lifecycle attention to training data, validation, monitoring, human override, audit logging and retirement criteria [22,35–38]. In the Saudi context, these requirements align with SDAIA's responsible AI principles and with PDPL-aware governance expectations.

This literature base supports the paper's central premise: a cybersecurity dashboard becomes strategically meaningful only when data, models, roles, controls, and decisions

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

are connected. A dashboard is therefore not a resilience mechanism by itself; it may support resilience when embedded within reliable telemetry, governed data curation, validated AI analytics, human-in-the-loop authority, machine-readable evidence and tested response procedures.

3. Methodology / Materials and Methods

This study uses a PRISMA-informed narrative evidence synthesis to support design-science artefact development. It is not a meta-analysis, statistical modelling study, or deployed-system evaluation. The scope is limited to sources relevant to AI/security analytics, cybersecurity governance, cyber-resilience, dashboards, critical infrastructure and Saudi digital governance.

Searches were documented on 09 July 2026 across Scopus, Web of Science, IEEE Xplore, ScienceDirect, ACM Digital Library and official policy/regulatory sources. The search used four concept blocks: AI/security analytics; cybersecurity/SOC/SIEM; dashboard/governance/evidence; and Saudi Arabia/Vision 2030/critical infrastructure. Sources were included when they addressed at least two of the core domains and were peer-reviewed, official policy/regulatory artefacts or reputable reports used only for contextual risk framing. Purely promotional sources, duplicative policy summaries and papers outside the dashboard-governance-security nexus were excluded.

Screening, coding, and qualitative appraisal were performed by one reviewer. No Cohen's kappa, Krippendorff's alpha or percentage-agreement statistic is reported. This is an explicit limitation. To compensate, the manuscript provides transparent search logic, decision rules, evidence classes, quality criteria, and data-extraction fields. The original core synthesis retained 18 sources; 13 additional high-relevance peer-reviewed or

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

foundational sources were later added to strengthen the paper's grounding in SOC maturity, SIEM/security analytics, cyber-resilience, AI assurance, critical-infrastructure protection and cybersecurity governance.

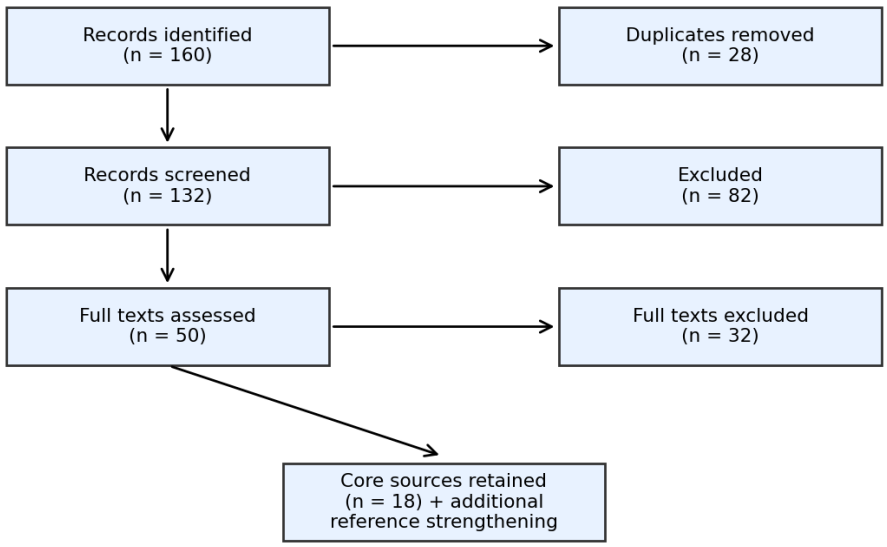

Figure 1. PRISMA-informed identification, screening and inclusion flow.

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

Table 1. Evidence hierarchy and use in the manuscript.

Evidence class	High-quality criteria	Use in paper
Peer-reviewed empirical	Transparent method, data and analysis	Supports empirical or adoption-related context
Peer-reviewed conceptual/review	Clear framework logic and references	Supports theory and framework development
Official policy/regulatory	Authoritative and current public document	Supports policy and control context
Industry threat report	Clear scope and timely evidence basis	Contextual urgency only, not effectiveness proof
Market forecast	Transparent publisher and scope	Context only
Author-prior work	Published or traceable and anonymized when required	Background only

4. Results

The synthesis produced seven design artefacts: (1) a typology of dashboard types, (2) a five-layer reference architecture, (3) a sectoral applicability matrix, (4) an operational threat-to-control mapping, (5) an AI model-governance and validation matrix, (6) a KPI dictionary and (7) a Responsible-AI implementation matrix. These results are intended as design artefacts for future validation rather than empirical performance findings.

Table 2. Dashboard typology and decision function.

Dashboard type	Primary users	Decision function	Evidence dependency
SOC operational dashboard	SOC analysts and incident handlers	Detect, triage and coordinate incidents	SIEM/SOAR events, endpoint, network and identity telemetry

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

Dashboard type	Primary users	Decision function	Evidence dependency
Executive cyber-risk dashboard	CISO, board and executive risk owners	Understand risk posture, appetite and priorities	Aggregated KPIs, trends and risk exceptions
Compliance/GRC evidence dashboard	Audit and compliance teams	Demonstrate control implementation and audit readiness	Control evidence, attestations and access reviews
AI model-governance dashboard	AI governance office and model owners	Monitor drift, explainability, false positives and review status	Model cards, validation logs, drift metrics and overrides
National/sector posture dashboard	Regulator or sector coordinator	Assess aggregated posture and resilience	Anonymized indicators and regulatory evidence

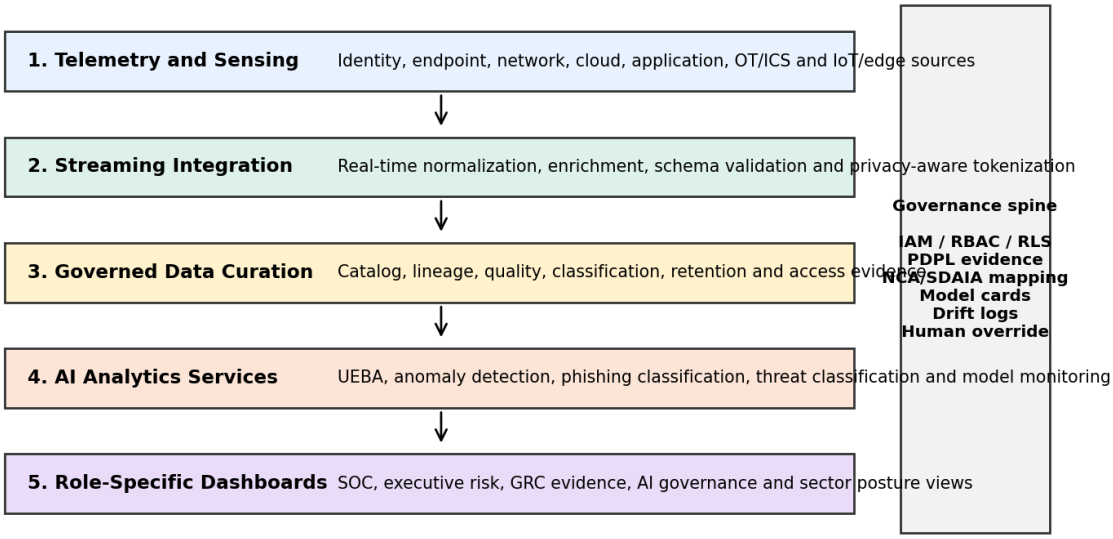

Figure 2. Real-time AI-driven cybersecurity analytics dashboard reference architecture.

The architecture contains telemetry and sensing, streaming integration, governed data curation, AI analytics services, and role-specific dashboards. A cross-cutting governance spine enforces IAM, RBAC/RLS, PDPL evidence, NCA/SDAIA mapping, model cards,

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

drift logs and human override. The architecture makes implementation dependencies explicit and avoids treating visualization as a substitute for resilience engineering.

Table 3. Sectoral applicability matrix for critical infrastructure.

Sector archetype	Telemetry sources	AI analytics priorities	Dashboard levels
IT-heavy services	Identity, endpoint, email, cloud and application logs	Credential abuse, phishing and anomalous access	SOC, CISO, GRC and executive risk
OT/ICS-heavy sectors	SCADA/ICS, PLC, sensor data and network flows	Segmentation violations, command deviation and anomaly detection	SOC/OT, plant leadership, CISO and regulator
Cloud-native government services	Cloud audit logs, APIs, identity federation and service metrics	API abuse, identity anomalies and service degradation	Service owner, SOC, GRC and digital-government leadership
Hybrid smart-city infrastructure	IoT, geospatial feeds, mobility platforms and edge gateways	Cross-domain correlation and disruption prediction	City operations, SOC, executive and sector posture
Food and agricultural infrastructure	ERP, supply-chain, production, logistics and quality systems	Supply disruption, identity anomalies and production anomalies	Operations, SOC, GRC and executive risk

Table 4. Operational threat-to-control taxonomy.

Threat vector	Control family / logic	Telemetry required	Detection logic	Response workflow	KPI / owner
AI-assisted phishing	Initial access; email security	Email headers, URLs and identity events	NLP classifier, URL reputation and risky-login correlation	Quarantine, notify and reset credentials when needed	Precision; SOC
Credential theft	Credential access; IAM; MFA	IdP logs, MFA events, session and geo/device data	UEBA, impossible travel and token replay detection	Revoke session, reset credentials and isolate endpoint	MTTD; IAM owner
Ransomware	Execution, lateral movement and impact	EDR, file changes,	Rapid file-change anomaly and	Isolate hosts, block C2 and	MTTR; SOC

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

Threat vector	Control family / logic	Telemetry required	Detection logic	Response workflow	KPI / owner
		SMB/RDP and privilege logs	lateral movement path detection	trigger recovery playbook	
Edge exploitation	Exposure and network security	VPN logs, firewall logs and vulnerability scans	Exploit attempt correlated with asset criticality	Patch, block source and rotate credentials	Closure time; network owner
Fileless malware	Defense evasion and endpoint controls	Memory telemetry, process tree and command logs	Abnormal script/process sequence detection	Terminate process, isolate endpoint and preserve artefacts	Containment time; endpoint owner
APT pre-positioning	Persistence, discovery and exfiltration	Identity, DNS, proxy and data-access logs	Low-and-slow anomaly correlation plus threat intelligence	Threat hunt and evidence preservation	Dwell-time estimate; CISO

Table 5. AI model governance and validation requirements.

Governance area	Implementation requirement	Evidence artefact	Dashboard indicator
Training data	Document source systems, labels, imbalance and privacy treatment	Dataset card and lineage record	Dataset freshness
Validation and calibration	Back-testing, precision/recall and false-positive/negative review	Validation report and threshold record	Confirmed alert rate
Concept/adversarial drift	Monitor distribution shift and adversary behavior change	Drift log and retraining trigger	Drift score
Explainability	Provide analyst-readable reasons for high-risk alerts	Model card and explanation log	Percentage of explained alerts
Human override	Permit documented confirmation, suppression and escalation	Override log and approval record	Override rate

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

Governance area	Implementation requirement	Evidence artefact	Dashboard indicator
Red-team testing	Test detection logic against simulated attack paths	Red-team report and ATT&CK coverage map	Coverage by tactic/technique
Audit logging	Record input, model version, output and human action	Immutable audit trace	Audit-ready model decisions
Retirement criteria	Retire unstable, unsupported or high-noise models	Retirement decision log	Models overdue for review

Table 6. KPI dictionary for real-time cyber-analytics dashboards.

KPI	Formula / definition	Data source	Frequency	Owner
MTTD	Average time from first observable event to confirmed alert	SIEM/EDR timestamps	Real-time/daily	SOC manager
MTTR	Average time from confirmed alert to containment or closure	SOAR/incident records	Daily/weekly	Incident response lead
Telemetry coverage	Instrumented critical assets / total critical assets × 100	CMDB and ingestion logs	Weekly	Asset owner
Evidence automation	Controls with machine evidence / in-scope controls × 100	GRC platform	Monthly	GRC owner
False-positive ratio	False positives / AI-generated alerts reviewed	SOC disposition logs	Weekly	Model owner
Model drift score	Performance or distribution shift against baseline	Model monitoring logs	Continuous/weekly	AI governance owner
Skills coverage	Staff meeting required competency	HR/certification records	Quarterly	Workforce owner

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

KPI	Formula / definition	Data source	Frequency	Owner
	baseline / role population × 100			

Table 7. Responsible AI implementation matrix.

Principle	Technical implementation	Governance owner	Evidence artefact
Fairness	Review alert impact across roles or groups were lawful and ethical	Responsible-AI office	Fairness review note
Privacy and security	PDPL-aware minimization, tokenization and access control	Data protection officer / CISO	Impact note and access log
Reliability and safety	Validation, staged deployment and rollback	Model owner / SOC manager	Validation and rollback record
Transparency	Model cards and analyst-readable explanations	AI governance lead	Model card and explanation log
Accountability	Defined decision rights and override authority	CISO / GRC owner	RACI and override logs
Human-centricity	Human-in-the-loop for high-impact containment	Incident response lead	Approval record
Social/environmental benefit	Proportional processing and service continuity	Executive risk owner	Benefit-risk assessment

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

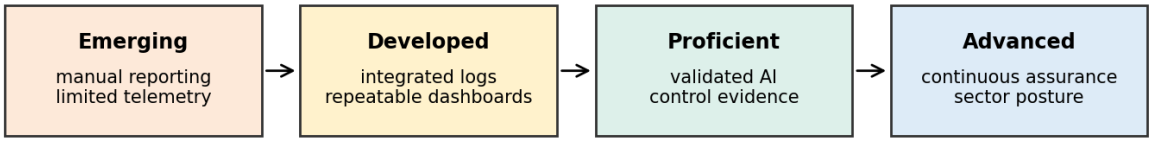

Figure 3. Cyber-analytics dashboard maturity model.

5. Discussion

The proposed framework advances three arguments. First, dashboards must be decomposed by purpose because SOC, executive risk, GRC evidence, AI-governance and sector posture views differ in audience, cadence, authority, and evidence. Treating all of these functions as a single dashboard would overstate visualization and understate the operational dependencies that produce cyber-resilience.

Second, the Saudi regulatory and policy environment strengthens the regional applicability of the framework but limits direct external validity. NCA, SDAIA, NDMO and PDPL mappings are Saudi-specific. The broader architecture—telemetry, integration, governed curation, AI analytics, role-specific dashboards and human decision rights—is transferable to other jurisdictions only if control mappings, privacy requirements and reporting rules are localized.

Third, framework effectiveness is conditional. Real-time dashboards may support cyber-resilience when telemetry coverage; AI model validation, human decision rights, machine-

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

readable evidence and tested response workflows are implemented together. Without these dependencies, dashboards risk becoming managerial reporting layers rather than decision infrastructure. This distinction is important because the manuscript is conceptual and has not been validated through deployment, simulation, Delphi review, or controlled expert evaluation.

6. Conclusion

This paper developed a PRISMA-informed design-science framework for real-time AI-driven cybersecurity analytics dashboards under Saudi Vision 2030. It clarified the contribution type, strengthened methodological transparency, expanded the reference base, separated dashboard functions, deepened AI model governance, operationalized threat-to-control mapping and provided KPI and Responsible-AI instruments. The framework is not empirical proof of improved cyber-resilience. Rather, it is a structured, auditable, and policy-aligned design that may support resilience when implemented and validated through reliable telemetry, governed AI models, human oversight, compliance evidence, and tested response workflows.

Future research should conduct expert validation with SOC managers, GRC officers, AI governance specialists and critical-infrastructure architects; apply structured scoring against relevance, completeness, feasibility and clarity; pilot the framework in one sector archetype; measure before/after KPIs; and refine the artefacts based on practitioner and executive feedback.

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

Acknowledgements

The author acknowledges the editorial and reviewer feedback that helped improve the methodological transparency, theoretical positioning, and operational clarity of the manuscript.

Funding

No external funding was received for this research.

Conflicts of Interest

The author declares no conflict of interest.

Author Responsibility Statement

The author confirms substantial contributions to the conception, design, synthesis, interpretation, and writing of the manuscript. The author approves the final version and agrees to its submission to the Nexus Science Review.

References

[1] Saudi Data & AI Authority (SDAIA). National Strategy for Data & AI (NSDAI). SDAIA, 2020/2025.

[2] SDAIA. SDAIA and Vision 2030. SDAIA, 2025.

[3] Saudi Press Agency. Saudi Arabia Emerges as AI Powerhouse under Vision 2030; 2026 Declared Year of Artificial Intelligence. SPA, 2026.

[4] SDAIA. AI Adoption Framework and AI Ethics Principles. SPA/SDAIA, 2024.

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

[5] National Cybersecurity Authority (NCA). Regulatory Framework: Essential Cybersecurity Controls, Saudi Cybersecurity Workforce Framework and AI Cybersecurity Guidelines. NCA, 2024–2026.

[6] Ahmad, M. Saudi Arabia's Cybersecurity Strategy in the AI Era: NCA, Critical-Infrastructure Protection, and Talent Development. 2025.

[7] CYFIRMA. Converging Threat Vectors: Escalating Cyber Risk and Strategic Exposure in Saudi Arabia's Digital Ecosystem (2025–2026). 2026.

[8] Fortinet. 2025 Global Cybersecurity Skills Gap Report—Saudi Arabia insights. 2025.

[9] Ken Research. Saudi Arabia AI in Cybersecurity Market, 2023–2030. 2025.

[10] Abudaqqa, F. Artificial Intelligence for IT Governance in Saudi Arabia within COBIT 2019 and ISO/IEC 38500 Frameworks. European Scientific Journal, 21(25), 125, 2025. DOI: 10.19044/esj.2025.v21n25p125.

[11] Cherukat, S. AI Strategy as a National Priority: A Governance-to-Execution Framework for Saudi Arabia Led by SDAIA (2020–2026). IJFMR, 2026.

[12] Alshammari, M. M., & Al-Mamary, Y. H. Building Trust and Cybersecurity Awareness in Saudi Arabia: Drivers of AI-Powered Smart-Home Device Adoption. Systems, 13(10), 863, 2025. DOI: 10.3390/systems13100863.

[13] Navigating the Cyber Landscape: Saudi Arabia's Cybersecurity Standards under Vision 2030. Arabian Journal for Science and Engineering, 2025. DOI: 10.1007/s13369-025-10765-y.

[14] Albaroudi, E., et al. Data Sovereignty and Digital Health Transformation in Saudi Arabia: Policy Implications for Vision 2030. Asian Journal of Research in Computer Science, 18(10), 115–135, 2025.

[15] Ouahchi, S. A National Big Data Governance Framework for Digital Government Transformation in Saudi Arabia. IRE Journals, 2026.

[16] Mazhar, C. B. National-Scale Data Governance Dashboards: Real-Time Quality, Lineage, Access, and Compliance for Saudi Arabia (SDAIA-Aligned). 2026.

[17] Mazhar, C. B. Smart City Real-Time Command Center: IoT Sensor Fusion, Lakehouse Analytics & Executive Dashboards for Riyadh/Jeddah. 2026.

[18] Mazhar, C. B. NEOM-Style Digital Infrastructure Analytics: Integrating 5G, IoT & Green Data Centers for Real-Time Governance and Sustainability. 2026.

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

[19] Hevner, A. R., March, S. T., Park, J., & Ram, S. Design Science in Information Systems Research. MIS Quarterly, 28(1), 75–106, 2004. DOI: 10.2307/25148625.

[20] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45–77, 2007. DOI: 10.2753/MIS0742-1222240302.

[21] Pascoe, C., Quinn, S., & Scarfone, K. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024. DOI: 10.6028/NIST.CSWP.29.

[22] Tabassi, E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1, 2023. DOI: 10.6028/NIST.AI.100-1.

[23] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160 Vol. 2 Rev. 1, 2021. DOI: 10.6028/NIST.SP.800-160v2r1.

[24] MITRE. Enterprise tactics and techniques. MITRE ATT&CK knowledge base, current version accessed 2026.

[25] ISO/IEC. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO, 2022.

[26] Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. Security Operations Center: A Systematic Study and Open Challenges. IEEE Access, 8, 227756–227779, 2020. DOI: 10.1109/ACCESS.2020.3045514.

[27] SOC Metrics and Performance Measurement. IEEE Xplore, 2025.

[28] López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. Systematic review of SIEM technology: SIEM-SC birth. International Journal of Information Security, 2023. DOI: 10.1007/s10207-022-00657-9.

[29] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 21(14), 4759, 2021. DOI: 10.3390/s21144759.

[30] Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. Electronics, 14(11), 2252, 2025. DOI: 10.3390/electronics14112252.

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 10/06/2026 - **Accepted:** 12/07/2026
Vol: 01.02
DOI: 10.66104/berfcb18
Pages: 1-18

[31] Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. A systematic review of cyber-resilience assessment frameworks. Computers & Security, 97, Article 101996, 2020. DOI: 10.1016/j.cose.2020.101996.

[32] Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. Applied Sciences, 14(24), 11807, 2024. DOI: 10.3390/app142411807.

[33] Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. The Resilience of Critical Infrastructure Systems: A Systematic Literature Review. Energies, 14(6), 1571, 2021. DOI: 10.3390/en14061571.

[34] Hilger, R. P. From cybersecurity to cyber resilience: a systemic and scalable approach for improving resilience and adaptive capacity. Journal of Cybersecurity, 12(1), tyag011, 2026. DOI: 10.1093/cybsec/tyag011.

[35] Nastoska, A., Jancheska, B., Rizinski, M., & Trajanov, D. Evaluating Trustworthiness in AI: Risks, Metrics, and Applications Across Industries. Electronics, 14(13), 2717, 2025. DOI: 10.3390/electronics14132717.

[36] Review of AI assurance: towards trustworthy, explainable and accountable AI. AI & Society, 2023. DOI: 10.1007/s00146-023-01802-1.

[37] Achuthan, K., Ramanathan, S. R. S., Srinivas, S., & Raman, R. Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. Frontiers in Big Data, 7, 2024. DOI: 10.3389/fdata.2024.1497535.

[38] Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. Information security governance in the public sector: investigations, approaches, measures, and trends. International Journal of Information Security, 2025. DOI: 10.1007/s10207-025-01097-x.

DOI: To be assigned by the journal