



Cyber Resilience Maturity Model for Multi-Site Construction and Energy Enterprises in Saudi Arabia under Vision 2030

Hafiz Shoaib Bashir^{1*}

¹Independent Researcher

*Corresponding Author

Hafiz Shoaib Bashir

Independent Researcher

Article History

Received: 27.07.2026

Accepted: 19.09.2026

Published: 22.09.2026

Abstract: Saudi Arabia's Vision 2030 is accelerating the digital integration of construction programmes, energy assets, cloud platforms, industrial control systems, and geographically dispersed project sites. This integration creates operational value but also expands the number of pathways through which cyber events can disrupt safety, productivity, data integrity, and service continuity. Existing cybersecurity frameworks provide strong control baselines, yet they do not fully express how a multi-site enterprise should measure resilience when temporary construction networks, contractor identities, common data environments, operational technology, remote access, and central security operations coexist. This review therefore develops a Cyber Resilience Maturity Model for multi-site construction and energy enterprises in Saudi Arabia. Evidence published between 2020 and 2025 was synthesized from peer-reviewed construction, industrial control, cyber-physical, and power-system research together with Saudi and international control frameworks. The review translates recurring evidence into eight maturity dimensions: governance and regulatory alignment; asset, identity, and architecture visibility; IT/OT segmentation and secure access; third-party and project supply-chain security; detection and security operations integration; incident response and cyber-physical recovery; workforce and contractor competence; and metrics, assurance, and adaptive improvement. Five maturity levels are proposed, progressing from fragmented practice to adaptive resilience. A criticality-weighted cross-site scoring method and minimum capability gates are introduced to prevent strong corporate controls from masking weaknesses at high-consequence locations. It provides Saudi enterprises with a practical basis for comparing sites, prioritizing investment, and linking cybersecurity improvement to continuity, safety, and Vision 2030 delivery.

Keywords: Cyber resilience; maturity model; construction cybersecurity; operational technology; multi-site enterprise; Saudi Arabia; Vision 2030; critical infrastructure.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

1. INTRODUCTION

Saudi Arabia is pursuing simultaneous expansion in infrastructure, industrial capacity, energy diversification, smart assets, and digital government under Vision 2030. Large construction and energy enterprises increasingly operate as

networks of corporate offices, engineering centres, project sites, plants, substations, warehouses, camps, cloud services, and specialist suppliers. Corporate enterprise systems may be centrally governed, while construction sites are formed rapidly, depend on temporary connectivity, and change their workforce

Citation: Bashir, H. S. (2026). Cyber Resilience Maturity Model for Multi-Site Construction and Energy Enterprises in Saudi Arabia under Vision 2030; *Glob Acad J Econ Buss*, 8(5), 1334-1344. <https://doi.org/10.36348/gajeb.2026.v08i05.025>

and subcontractor population throughout the project lifecycle. Energy sites add operational technology (OT), supervisory control and data acquisition, protection systems, engineering workstations, safety systems, and long-lived field devices whose availability requirements differ materially from conventional information technology. Vision 2030 therefore increases the importance of cyber resilience as a property of the enterprise system, not merely the security of individual devices or applications [1-6].

Cybersecurity and cyber resilience are related but distinct. Security controls seek to reduce the likelihood and impact of compromise; resilience additionally asks whether essential operations can anticipate, withstand, recover from, and adapt after adverse cyber conditions. The distinction is especially important in construction and energy environments because complete prevention is unrealistic when enterprises contain heterogeneous legacy assets, contractors, remote sites, cloud dependencies, mobile equipment, and changing project interfaces. The NIST Cybersecurity Framework 2.0 formalizes Govern alongside Identify, Protect, Detect, Respond, and Recover, while the U.S. Department of Energy Cybersecurity Capability Maturity Model organizes improvement as institutionalized practices rather than isolated technical controls [7,8]. Guidance for OT further emphasizes architecture, safety, availability, controlled remote access, monitoring, and recovery that respect physical-process constraints [9].

The National Cybersecurity Authority's Essential Cybersecurity Controls establish enterprise-wide requirements, while the Operational Technology Cybersecurity Controls extend protection to industrial and critical operational environments [1,2]. Data and cloud controls add requirements relevant to common data environments, analytics platforms, hosted applications, and project collaboration services [3,4]. The implementation guide for OT controls reinforces the need to translate high-level obligations into repeatable operational practices [5]. These instruments specify what must be controlled, but a multi-site organization still needs a way to determine whether those controls are consistently embedded across locations, whether weak sites are visible to leadership, and whether incident recovery can be coordinated when IT and OT dependencies span several facilities.

Digital construction increasingly depends on building information modelling (BIM), common data environments, connected sensors, drones, mobile platforms, digital twins, and remotely supported equipment. Studies identify fragmented

responsibility, weak cybersecurity awareness, temporary networks, supply-chain dependence, and uncertainty over ownership of cyber risk as recurring problems [16-24]. Energy and industrial research reports parallel concerns around IT/OT convergence, insecure industrial protocols, remote engineering access, asset visibility, cyber-physical consequences, and recovery under conditions where shutdown itself may create safety or production risk [25-30]. Generic enterprise maturity scores can therefore be misleading if they average a well-controlled corporate centre with a poorly segmented plant or a rapidly mobilized project site.

The aim of this review is to synthesize recent evidence and develop a Cyber Resilience Maturity Model (CRMM) tailored to multi-site construction and energy enterprises operating in Saudi Arabia. First, it characterizes the cyber-resilience exposure created by distributed construction and energy operating models. Second, it consolidates Saudi regulatory expectations with internationally recognized resilience and maturity practices. Third, it derives domain-specific maturity dimensions and observable indicators suited to both temporary and permanent sites. Fourth, it formulates a cross-site scoring logic that accounts for unequal site criticality and prevents aggregation from hiding severe local deficiencies. Fifth, it identifies implementation priorities and research needs that can support resilient delivery of Vision 2030 programmes. The contribution is a review-derived management architecture that connects compliance, cyber-physical continuity, and measurable organizational learning.

2. MATERIALS AND METHODS

This study uses a structured integrative review and multi-criteria synthesis. The method was selected because the research problem spans distinct evidence communities: construction cybersecurity, industrial control and energy resilience, organizational maturity models, Saudi cybersecurity regulation, and international control standards. The analysis therefore treats the maturity model as a synthesis problem in which recurring requirements are identified, compared, and translated into observable enterprise capabilities.

The review window was limited to 2020-2025 to reflect current digital construction practices, contemporary OT threats, and recent control-framework revisions. Peer-reviewed evidence was considered when it addressed at least one of the following: cybersecurity in construction projects or digital built environments; industrial control systems or power-system cyber resilience; digital twins and cyber-physical risk; third-party or supply-chain exposure; organizational cybersecurity capability;

incident response, continuity, or recovery. Authoritative institutional sources were included where they defined applicable controls or maturity concepts. These sources comprised National Cybersecurity Authority documents, the Vision 2030 annual reporting framework, NIST publications, the DOE capability model, ISO/IEC information-security standards, IEC industrial automation requirements, CISA performance goals, and European supply-chain guidance [1-15].

Sources were excluded when they predated 2020, focused exclusively on cryptographic algorithms without enterprise-resilience implications, described isolated attack detection without organizational or operational context, duplicated a later version of a standard, or lacked sufficient methodological or institutional credibility. Instead, evidence was coded according to its relevance to multi-site operations and its ability to define a capability that could be observed or assessed.

First, recurring exposures were extracted from the literature and grouped into governance, technology, operational, human, and inter-organizational categories. Second, the exposures were mapped against Saudi and international controls to distinguish regulatory obligations from maturity-enhancing practices. Third, overlapping requirements were consolidated into eight CRMM dimensions. Fourth, each dimension was expressed through maturity characteristics that progress from

local, reactive activity toward standardized, measured, and adaptive enterprise practice.

The proposed model uses five levels: Level 1 Fragmented, Level 2 Repeatable, Level 3 Standardized, Level 4 Measured, and Level 5 Adaptive. For enterprise aggregation, the review proposes a criticality-weighted Cyber Resilience Maturity Index. For site s and maturity dimension d , the assessed score M_{sd} ranges from 1 to 5, w_d is the dimension weight, and C_s is the normalized criticality weight of the site. The enterprise index is calculated as the sum of C_s multiplied by the weighted site score, divided by the sum of site criticalities. Criticality can reflect safety consequence, production dependency, regulatory significance, data sensitivity, recovery time objective, and network centrality. This prevents a large number of low-risk offices from numerically overwhelming a small number of high-consequence OT or flagship construction sites.

An enterprise cannot be rated at Level 4 or Level 5 if any high-criticality location remains below Level 3 in identity control, OT/IT segmentation, incident response, or recoverability. The gate reflects the systemic nature of multi-site operations: one unmanaged vendor pathway, flat OT boundary, or untested recovery process can become the route through which an otherwise mature organization experiences enterprise-wide disruption.

$CRMI = [\sum_s C_s (\sum_d w_d M_{s,d})] / \sum_s C_s$
where C_s is site criticality, w_d is the domain weight, and $M_{s,d}$ is the site-domain maturity score.

Table 1: Evidence-to-model synthesis used to derive the CRMM

Evidence stream	Recurring multi-site issue	CRMM requirement	Principal sources
Saudi regulatory controls	Enterprise, OT, data and cloud obligations must remain traceable across locations.	Governance, risk classification, control ownership and regulatory mapping.	[1-5]
Construction cybersecurity	Temporary networks, BIM/CDE, commissioning, fragmented ownership and contractor churn.	Lifecycle-aware asset, identity, supplier and handover controls.	[16-24]
Energy / industrial control	IT/OT convergence, legacy assets, safety constraints, remote engineering and cyber-physical impact.	Segmentation, secure remote access, OT-aware monitoring and trusted recovery.	[2,5,9,25-30]
Capability frameworks	Control presence alone does not show institutionalization or measured performance.	Five cumulative maturity levels with evidence-based progression.	[7,8,11-14]
Supply-chain guidance	Risk crosses organizational boundaries through OEMs, subcontractors and digital platforms.	Tiered supplier assurance, access lifecycle and coordinated incident obligations.	[15-18]

3. Multi-Site Threat Surface in Construction and Energy

Each additional location introduces local users, devices, access methods, suppliers, and operational priorities, yet the locations are

commonly joined through shared identity services, cloud tenants, enterprise resource planning, remote support, security tooling, or wide-area networks. A compromise at a small site can therefore acquire strategic significance when credentials, trust

relationships, or management channels are reused. Zero-trust architecture is relevant because it shifts emphasis from implicit network location to explicit verification of identity, device, and context [10]. However, zero trust in construction and energy cannot be implemented as a single product; it requires accurate inventories, least-privilege design, segmentation, authentication, logging, and lifecycle discipline across changing populations of people and assets.

They are mobilized quickly, evolve through design, enabling works, main construction, testing, commissioning, handover, and demobilization, and can include hundreds of firms with unequal security capability. Temporary offices may use consumer-grade connectivity, personal or subcontractor-managed devices, portable storage, ad hoc wireless links, and rapidly deployed cameras or sensors. BIM and common data environments concentrate commercially sensitive models, design revisions, approvals, and access permissions. Digital twins and connected site systems increase the value of data integration but also expand dependencies between physical progress and digital availability [16,20,23]. Survey and framework studies in construction repeatedly identify fragmented governance and limited awareness as material weaknesses, indicating that maturity must include responsibility and behavior rather than only technical controls [16-19].

During this phase, project networks, original-equipment-manufacturer laptops, temporary remote connections, building-management systems, industrial devices, and enterprise services can coexist before final ownership boundaries are fully established. Credentials created for testing can persist into operation, while asset registers may not capture last-minute substitutions or firmware states. Research on BIM/CDE environments and construction networks shows that connected collaboration and operational technologies introduce vulnerabilities that are difficult to manage if cyber requirements are introduced late [19,21,24]. A maturity model should consequently evaluate secure-by-design procurement, commissioning controls, asset transfer, and removal of temporary access as lifecycle capabilities.

Industrial control systems frequently contain specialized protocols, vendor-specific devices, legacy operating systems, and equipment that cannot be patched on normal IT schedules. Bhamare *et al.*, describe the security implications of increased connectivity between ICS, cloud services, and enterprise networks, while later industrial-resilience research emphasizes the need to anticipate, withstand, recover, and adapt rather than

assume prevention alone [25,26]. NIST OT guidance likewise stresses that security measures must respect performance, reliability, and safety requirements [9]. In power and energy settings, cyber events can influence measurement, control, protection, dispatch, or availability, creating effects that may propagate beyond information loss.

Cyber-physical resilience depends on understanding interdependence between communications, control functions, physical assets, and human decisions [28]. Power-electronics-enabled systems add digitally controlled converters and distributed components whose observability and controllability depend on communication infrastructure, increasing the importance of before-during-after resilience measures [29]. Industrial cyber-resilience reviews similarly argue for layered strategies that combine prevention, detection, response, and recovery [26]. These findings imply that an enterprise maturity model should assess not only whether security technologies exist, but also whether the organization can maintain essential functions in degraded conditions, isolate affected zones, restore trusted states, and learn across sites.

Construction projects rely on designers, subcontractors, equipment suppliers, platform providers, commissioning specialists, and temporary labour. Energy operations rely on original equipment manufacturers, maintenance contractors, system integrators, telecom providers, cloud services, and specialist engineering support. Supply-chain guidance emphasizes governance, contractual requirements, visibility, assurance, and coordinated incident handling [15]. In a Saudi multi-site context, third-party maturity must also include rapid onboarding and offboarding, privileged remote access, subcontractor device control, ownership of logs, and evidence that suppliers can support recovery.

4. Review-Derived Cyber Resilience Maturity Model

The CRMM consolidates the evidence into eight dimensions that can be applied consistently across corporate, construction, and energy locations. Each represents a capability that must be governed, implemented, evidenced, and improved. They also provide a common language through which security teams, project directors, plant managers, engineering functions, procurement, and executive leadership can compare sites without assuming that every location uses identical technology.

The first dimension is governance, risk, and regulatory alignment. Mature resilience begins with accountable ownership, clear risk appetite, site classification, policy inheritance, exceptions

management, and traceability to applicable Saudi controls [1-5]. At Level 3, governance is standardized across business units and projects, with defined control owners and documented risk acceptance. The Govern function in CSF 2.0 and the institutionalization concept in C2M2 support this movement from documented intent to managed capability [7,8].

The second dimension is asset, identity, and architecture visibility. Resilience is impossible when organizations do not know which assets exist, who can access them, how systems depend on one another, or which connections are temporary. Construction inventories should include project applications, wireless devices, cameras, IoT sensors, drones, commissioning equipment, and cloud workspaces. Energy inventories must extend to controllers, engineering stations, historians, safety interfaces, communications equipment, and firmware or support status. Identity governance must cover employees, subcontractors, vendor engineers, machine identities, service accounts, and emergency credentials. NIST zero-trust principles reinforce continuous verification and least privilege, while OT guidance requires architecture awareness before controls can be safely changed [9,10].

The third dimension is IT/OT segmentation and secure access. Segmentation limits blast radius and creates enforceable trust boundaries between corporate systems, project networks, guest access, building systems, production zones, safety functions, and remote support. Maturity is evidenced by approved architecture patterns, controlled conduits, secure administrative paths, multifactor authentication where technically feasible, time-bounded vendor access, session recording for privileged activity, and periodic validation that firewall rules still reflect operational need. IEC 62443 asset-owner requirements provide a strong basis for security programme and zone/conduit thinking [13]. Saudi OT controls further require organizations to translate segmentation and access principles into local industrial practice [2,5].

The fourth dimension is third-party and project supply-chain security. This domain recognizes that multi-site resilience is partly determined by organizations that the enterprise does not directly manage. Maturity progresses from generic contractual clauses toward risk-tiered due diligence, minimum security requirements, identity lifecycle integration, technical access restrictions, supplier incident obligations, evidence-based assurance, and tested alternatives for critical dependencies. Construction projects require particular emphasis on subcontractor churn and transfer of digital assets at handover, while energy

sites require stronger governance of original-equipment-manufacturer remote support and maintenance channels. Supply-chain guidance and construction studies both show that accountability gaps become systemic when responsibilities are distributed [15-18].

The fifth dimension is detection and security operations integration. A mature enterprise can see meaningful security events across locations without forcing every site into identical telemetry. Corporate and cloud logs, identity events, endpoint alerts, network security data, OT monitoring, and selected physical-process indicators should be integrated according to site criticality. Lower maturity is characterized by local alerts and manual escalation. Standardized maturity establishes common use cases, time synchronization, retention, escalation paths, and a shared incident taxonomy. Measured maturity evaluates detection coverage, time to triage, false-positive burden, and visibility gaps. Adaptive maturity uses threat intelligence, lessons from incidents, and site-specific attack paths to refine analytics. CISA performance goals emphasize foundational logging and response practices, while OT research cautions that monitoring must be engineered to avoid disrupting control environments [9,14,25].

The sixth dimension is incident response and cyber-physical recovery. Plans must define decision authority, technical containment, operational fallback, communications, evidence preservation, recovery sequencing, and criteria for returning systems to trusted service. Construction recovery may prioritize access to current drawings, approvals, scheduling, commercial systems, and site communications. Energy recovery may require safe-state transitions, manual operations, redundant control paths, restoration of engineering workstations, validation of controller logic, and coordination with operational safety teams. Resilience literature stresses the full before-during-after lifecycle, making tested restoration and adaptation essential indicators [26,28,29].

The seventh dimension is workforce and contractor competence. Multi-site enterprises need role-based competence for site managers, engineers, administrators, procurement staff, commissioning teams, control-room personnel, and contractor supervisors. Mature organizations connect training to actual decision scenarios: handling suspicious remote-support requests, protecting privileged credentials, reporting lost field devices, validating changes to control logic, managing removable media, and escalating incidents without bypassing safety procedures. Construction studies consistently identify awareness and fragmented responsibility as

barriers [17,18]. A maturity assessment should therefore seek behavioral evidence, exercise participation, and supervisor reinforcement rather than training records alone.

The eighth dimension is metrics, assurance, and adaptive improvement. Evidence can include architecture reviews, vulnerability remediation by criticality, supplier assurance, exercise outcomes, backup restoration tests, access recertification, OT

rule reviews, response times, and repeat findings. At Level 4, metrics are used to compare sites and expose variation; at Level 5, trends and scenario evidence drive predictive changes to architecture, investment, and operating procedures. ISO/IEC 27001 and 27002 provide a management-system foundation for evaluation and improvement, while capability models emphasize repeatability and institutionalization [8,11,12].

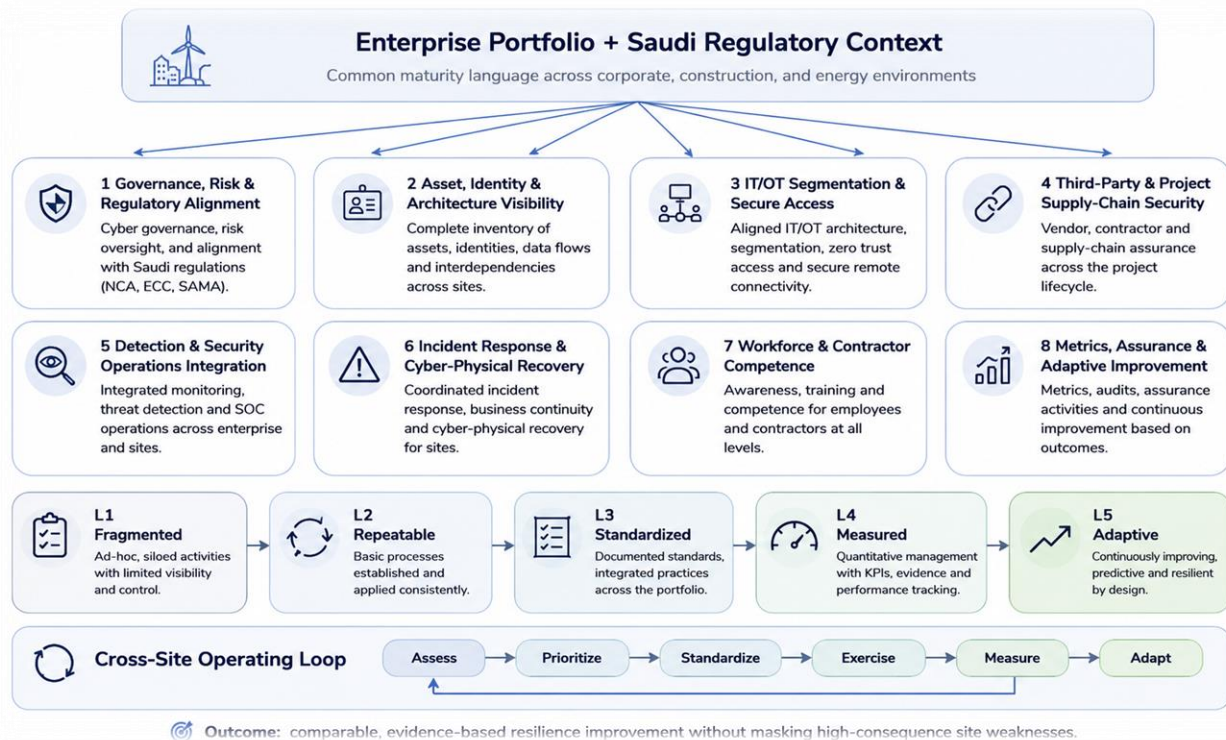


Figure 1: Review-derived Cyber Resilience Maturity Architecture for multi-site construction and energy enterprises

5. Maturity Levels and Cross-Site Assessment Logic

The five maturity levels describe how consistently the eight dimensions are embedded. Level 1, Fragmented, is characterized by local knowledge, reactive activity, undocumented exceptions, and dependence on individual expertise. Level 2, Repeatable, introduces basic procedures, named owners, recurring operational tasks, and initial inventories, although practices still vary by project or site. Level 3, Standardized, establishes approved enterprise patterns, common evidence requirements, defined lifecycle processes, and consistent minimum controls. Level 4, Measured, adds quantitative performance management, cross-site comparison, validated recovery, and systematic assurance. Level 5, Adaptive, uses threat intelligence, incident learning, scenario testing, and business change signals to adjust controls before weaknesses become systemic.

Standardization demonstrates that the enterprise has designed a consistent way of working; measurement demonstrates that it knows whether the design performs. A site may have a documented incident plan yet remain unable to restore critical services within operational tolerance. A Level 4 rating therefore requires operational evidence such as successful recovery tests, verified segmentation, identity recertification, measured detection coverage, supplier assurance outcomes, and trend-based remediation. Level 5 requires evidence that these measurements alter future decisions, for example changing a standard remote-access pattern after recurring vendor weaknesses are discovered.

Cross-site scoring should be conducted at the lowest organizational unit that can meaningfully own risk. For a large enterprise this may be an individual plant, major construction project, regional office, or shared digital platform. Each unit is scored across the eight dimensions using evidence defined in an

assessment workbook. Domain weights may be adjusted within a controlled governance process, but default weighting should keep governance, segmentation/access, detection, and response/recovery prominent because failures in these areas can propagate widely. Site criticality then determines how heavily the location influences the enterprise index. A producing energy facility or integrated control centre would normally receive greater criticality than a small administrative office; a flagship construction programme with extensive connected commissioning systems may rank higher than a conventional project site.

Averages can create a false impression of resilience when high scores at low-risk sites compensate for severe weaknesses at a critical facility. The proposed capability gates therefore impose minimum conditions. High-criticality sites must reach at least Standardized maturity in privileged identity, segmentation, incident response, and recoverability before the enterprise can claim Measured maturity. To claim Adaptive maturity, high-criticality sites should also demonstrate current exercises, closed material findings, tested supplier escalation, and evidence that lessons are shared

across the portfolio. The gates make the model deliberately conservative, reflecting the fact that resilience is constrained by dependencies and weakest trusted pathways.

Policy documents establish intent; technical configuration demonstrates implementation; logs and metrics show operation; interviews reveal actual decision pathways; exercises and recovery tests demonstrate performance. Construction sites may need observations during mobilisation and commissioning because a static audit can miss short-lived access paths. Energy locations may require carefully planned configuration reviews or passive validation to avoid operational disruption.

Executives can view the enterprise index and the distribution of site scores, while technical leaders can identify domains with systemic variance. A portfolio in which governance is mature but recovery is weak requires a different investment programme from one in which OT segmentation is strong but contractor identity remains uncontrolled. The model therefore supports prioritization by showing where maturity deficits coincide with high site criticality, regulatory exposure, or cross-site dependency.

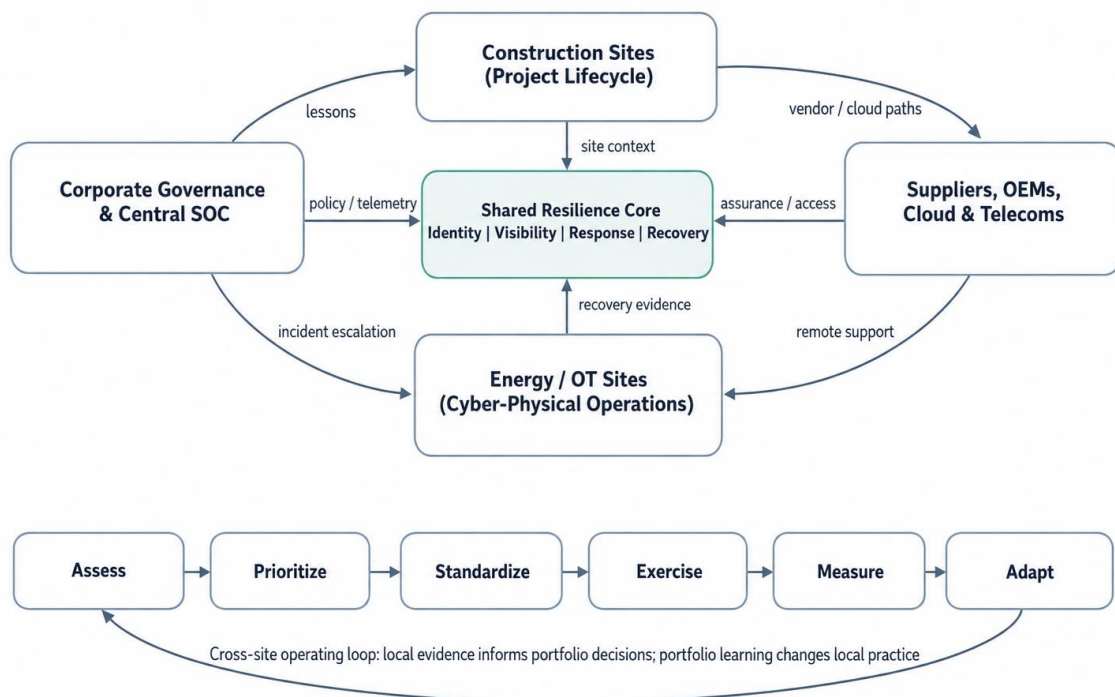


Figure 2: Cross-site cyber resilience operating loop linking central governance, construction sites, energy/OT sites and external dependencies

Table 2: Five-level maturity scale and assessment evidence

Level	Operating character	Typical evidence	Enterprise interpretation
1 - Fragmented	Reactive, local and person-dependent.	Partial inventories; informal access; incident activity depends on individuals.	Capability exists inconsistently and cannot be relied upon portfolio-wide.
2 - Repeatable	Basic procedures recur but differ by site or project.	Named owners; recurring tasks; initial supplier and access controls.	Some predictability, with material cross-site variation.
3 - Standardized	Common patterns and minimum controls are institutionalized.	Approved architectures; lifecycle processes; common evidence and escalation.	Minimum target for high-criticality gated capabilities.
4 - Measured	Performance is verified and compared across sites.	Recovery tests; detection coverage; access recertification; trend metrics.	Enterprise can demonstrate effectiveness, not merely documentation.
5 - Adaptive	Evidence, threats and lessons change future practice.	Scenario-driven changes; cross-site learning; predictive assurance and redesign.	Resilience is continually adjusted to business and threat change.

6. Implementation Priorities for Vision 2030 Enterprises

Implementation should begin with enterprise topology rather than a universal technology rollout. Organizations need a defensible register of sites, shared platforms, major suppliers, critical business services, and IT/OT interconnections. This portfolio view enables leadership to classify locations by consequence and identify common pathways that could allow a local compromise to become an enterprise event. Its purpose is to establish variation, expose evidence gaps, and identify high-criticality sites below capability gates rather than to produce an attractive average score.

The next priority is to standardize a small number of cross-site control patterns. Examples include contractor onboarding and offboarding, privileged remote access, project-network segmentation, OT vendor access, logging minimums, backup validation, and incident escalation. Standard patterns reduce the burden on project teams and plant engineers because they turn cybersecurity from bespoke interpretation into reusable engineering and operating requirements. For construction, these patterns should be embedded in procurement, mobilisation, commissioning, and handover documents. For energy, they should be incorporated into maintenance processes, management of change, outage planning, and vendor support agreements.

Enterprises often invest heavily in detection while assuming that backups equate to recoverability. The CRMM requires a stronger test: can a site restore the minimum technology and information needed to operate safely, and can corporate functions support that restoration when several locations are affected? Exercises should combine cyber and operational decisions, including loss of identity services, unavailable cloud platforms,

compromised engineering workstations, vendor unavailability, or corrupted project data. High-criticality sites should define minimum viable operating states and the evidence required before reconnecting restored systems. Recovery tests should also verify dependencies such as certificates, licensing servers, domain services, configuration repositories, telecoms, and clean administrative workstations.

A central security operations centre can provide scale, but it needs site context to interpret alerts correctly. OT alarms, construction-site network changes, contractor logins, or commissioning activity may be legitimate in one lifecycle phase and anomalous in another. Mature integration therefore combines centralized analytics with local operational knowledge and clear escalation authority. Detection use cases should be mapped to critical attack paths rather than simply maximizing log volume. Sites with limited telemetry should have compensating controls and a documented plan for improving visibility.

Finally, improvement should be linked to Vision 2030 delivery outcomes. Cyber resilience protects more than confidentiality: it supports schedule reliability, operational availability, worker and process safety, continuity of critical services, protection of intellectual property, and confidence in digital transformation. For example, stronger vendor access controls reduce both cyber exposure and uncertainty during commissioning; tested recovery protects production and project milestones; better asset visibility improves maintenance and cyber response simultaneously.

7. Critical Synthesis and Research Agenda

First, construction cybersecurity research has developed rapidly, yet much of it remains focused on identifying vulnerabilities, awareness deficits, or

digital-technology risks rather than validating longitudinal maturity models across live project portfolios [16-24]. Second, energy and industrial literature offers deeper treatment of cyber-physical resilience, but models are frequently device-, network-, or power-system-centric and may not include contractor churn, project lifecycle transitions, or enterprise governance [25-30]. The proposed CRMM bridges these bodies of evidence by treating multi-site resilience as a combined organizational and cyber-physical capability.

Saudi controls and international standards provide necessary baselines, but compliance status should not be interpreted as a direct measure of resilience. A control can be documented without being consistently implemented, implemented without being monitored, or monitored without being recoverable after failure. Maturity assessment adds a temporal and institutional dimension: it asks whether practices recur, whether performance is known, and whether the organization learns. Enterprises must retain traceability from model dimensions to mandatory controls, because a high maturity score in one domain cannot compensate for an unmet regulatory obligation in another.

Most maturity approaches assume one organizational boundary and do not explicitly address how to combine sites with very different consequences. Future work should test alternative criticality weights, gating rules, and statistical treatments using real enterprise portfolios. Researchers should examine whether maturity variance is itself a risk indicator, particularly where shared identity, networks, or suppliers connect sites. Longitudinal studies could determine whether reducing variance improves incident outcomes more effectively than raising the enterprise average.

Commissioning is a period in which temporary project practices become permanent operational dependencies, yet cybersecurity ownership can be ambiguous. Future studies should measure the persistence of temporary credentials, remote-access paths, unmanaged engineering assets, and incomplete inventories after handover. Comparable research is needed on how cyber requirements are transferred from project contracts into operating maintenance agreements.

Useful indicators may include time to revoke contractor access, percentage of critical assets with verified owners, recovery success under loss of central services, proportion of privileged vendor sessions monitored, detection coverage for defined attack paths, and closure time for cross-site lessons. These measures need validation against actual incident or exercise performance. Future studies

should also examine the balance between common enterprise metrics and sector-specific indicators, because excessive standardization can conceal the engineering realities of OT while excessive local tailoring prevents meaningful comparison.

Finally, the role of digital twins, artificial intelligence, and autonomous analytics deserves careful study. These technologies can improve visibility, anomaly detection, and scenario rehearsal, but they also introduce new dependencies, model integrity concerns, and concentrated data stores [20,22,23]. Mature enterprises should therefore assess them as both resilience enablers and assets requiring protection. Research should test whether digital replicas can support safe cyber-recovery rehearsals, how model trust can be validated after compromise, and how automated recommendations should be governed when decisions have physical safety consequences.

8. CONCLUSION

Saudi construction and energy enterprises are becoming more connected, distributed, and cyber-physical as Vision 2030 programmes scale. The evidence reviewed from 2020-2025 indicates that resilience cannot be inferred from the presence of security tools or from a single enterprise compliance score. Temporary construction networks, contractor ecosystems, common data environments, OT assets, remote engineering access, and shared digital platforms create dependencies through which local weaknesses can have portfolio-wide consequences.

This review develops a five-level Cyber Resilience Maturity Model organized around eight dimensions: governance and regulatory alignment; asset, identity, and architecture visibility; IT/OT segmentation and secure access; third-party and project supply-chain security; detection and security operations integration; incident response and cyber-physical recovery; workforce and contractor competence; and metrics, assurance, and adaptive improvement. The model combines a criticality-weighted enterprise index with minimum capability gates so that strong performance at low-risk locations cannot conceal material weakness at high-consequence sites.

The practical implication is that resilience improvement should be managed as a portfolio discipline. Enterprises should classify sites, standardize cross-site control patterns, integrate cybersecurity into project and asset lifecycles, test minimum viable recovery, and use evidence to compare capability rather than documentation alone. Its value lies in connecting those requirements to repeatable organizational maturity and cross-site operational resilience. With empirical validation, the

CRMM can provide a common basis for executive oversight, site-level improvement, supplier governance, and research on the cyber resilience of complex Saudi construction and energy ecosystems.

Data Availability Statement: No new empirical data were generated in this review. The proposed model is derived from the cited literature, standards, and institutional guidance.

Conflicts of Interest: The author(s) declare no conflict of interest.

REFERENCES

1. National Cybersecurity Authority (NCA). Essential Cybersecurity Controls (ECC 2-2024). Riyadh, Saudi Arabia, 2024.
2. National Cybersecurity Authority (NCA). Operational Technology Cybersecurity Controls (OTCC-1:2022). Riyadh, Saudi Arabia, 2022.
3. National Cybersecurity Authority (NCA). Data Cybersecurity Controls (DCC-1:2022). Riyadh, Saudi Arabia, 2022.
4. National Cybersecurity Authority (NCA). Cloud Cybersecurity Controls (CCC-2:2024). Riyadh, Saudi Arabia, 2024.
5. National Cybersecurity Authority (NCA). Guide to Operational Technology Cybersecurity Controls Implementation (GOTCC-1:2023). Riyadh, Saudi Arabia, 2023.
6. Saudi Vision 2030. Annual Report 2024. Riyadh, Saudi Arabia, 2025.
7. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, Gaithersburg, MD, 2024. doi:10.6028/NIST.CSWP.29.
8. U.S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2), Version 2.1. Washington, DC, 2022.
9. Stouffer, K.; Pease, M.; Tang, C.; *et al.*, Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3. National Institute of Standards and Technology, 2023. doi:10.6028/NIST.SP.800-82r3.
10. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST SP 800-207. National Institute of Standards and Technology, 2020. doi:10.6028/NIST.SP.800-207.
11. International Organization for Standardization. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. Geneva, 2022.
12. International Organization for Standardization. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Controls. Geneva, 2022.
13. International Electrotechnical Commission. IEC 62443-2-1:2024 Security for Industrial Automation and Control Systems - Security Program Requirements for IACS Asset Owners. Geneva, 2024.
14. Cybersecurity and Infrastructure Security Agency (CISA). Cross-Sector Cybersecurity Performance Goals. Washington, DC, 2023.
15. European Union Agency for Cybersecurity (ENISA). Good Practices for Supply Chain Cybersecurity. Athens/Heraklion, 2023.
16. Turk, Z.; Garcia de Soto, B.; Mantha, B.R.K.; Maciel, A.; Georgescu, A. A systemic framework for addressing cybersecurity in construction. *Automation in Construction* 2022, 133, 103988. doi:10.1016/j.autcon.2021.103988.
17. Garcia de Soto, B.; Turk, Z.; Maciel, A.; Mantha, B.R.K.; Georgescu, A.; Sonkor, M.S. Understanding the significance of cybersecurity in the construction industry: Survey findings. *Journal of Construction Engineering and Management* 2022, 148(9), 04022095. doi:10.1061/(ASCE)CO.1943-7862.0002344.
18. Mantha, B.R.K.; Garcia de Soto, B. Cybersecurity in construction: Where do we stand and how do we get better prepared. *Frontiers in Built Environment* 2021, 7, 612668. doi:10.3389/fbuil.2021.612668.
19. Sonkor, M.S.; Garcia de Soto, B. Operational technology on construction sites: A review from the cybersecurity perspective. *Journal of Construction Engineering and Management* 2021, 147(12), 04021172. doi:10.1061/(ASCE)CO.1943-7862.0002193.
20. Alshammari, K.; Beach, T.; Rezgui, Y. Cybersecurity for digital twins in the built environment: Current research and future directions. *Journal of Information Technology in Construction* 2021, 26, 159-173. doi:10.36680/j.itcon.2021.010.
21. Turk, Z.; Sonkor, M.S.; Klinc, R. Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. *Journal of Civil Engineering and Management* 2022, 28(5), 349-364. doi:10.3846/jcem.2022.16682.
22. Yao, D.; Garcia de Soto, B. Enhancing cyber risk identification in the construction industry using language models. *Automation in Construction* 2024, 165, 105565. doi:10.1016/j.autcon.2024.105565.
23. Parn, E.; Ghadiminia, N.; Garcia de Soto, B.; Oti-Sarpong, K. A perfect storm: Digital twins, cybersecurity, and general contracting firms. *Developments in the Built Environment* 2024, 18, 100466. doi:10.1016/j.dibe.2024.100466.
24. Mantha, B.R.K.; Sonkor, M.S.; Garcia de Soto, B. Investigation of the cyber vulnerabilities of construction networks using an agent-based model. *Developments in the Built Environment* 2024, 18, 100452. doi:10.1016/j.dibe.2024.100452.

25. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for industrial control systems: A survey. *Computers & Security* 2020, 89, 101677. doi:10.1016/j.cose.2019.101677.
26. Alrumaih, T.N.I.; Alenazi, M.J.F.; AlSowaygh, N.A.; Humayed, A.A.; Alablani, I.A. Cyber resilience in industrial networks: A state of the art, challenges, and future directions. *Journal of King Saud University - Computer and Information Sciences* 2023, 35(9), 101781. doi:10.1016/j.jksuci.2023.101781.
27. Xu, L.; Guo, Q.; Sheng, Y.; Muyeen, S.M.; Sun, H. On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. *Renewable and Sustainable Energy Reviews* 2021, 152, 111642. doi:10.1016/j.rser.2021.111642.
28. Hou, J.; Hu, C.; Lei, S.; Hou, Y. Cyber resilience of power electronics-enabled power systems: A review. *Renewable and Sustainable Energy Reviews* 2024, 189, 114036. doi:10.1016/j.rser.2023.114036.
29. Harkat, H.; Camarinha-Matos, L.M.; Goes, J.; Ahmed, H.F.T. Cyber-physical systems security: A systematic review. *Computers & Industrial Engineering* 2024, 188, 109891. doi:10.1016/j.cie.2024.109891.
30. Qureshi, A.R.; Alhumyani, H.; Alqurashi, F.; Aljuaid, H. Digital twin-based cybersecurity framework for smart manufacturing systems. *Future Generation Computer Systems* 2024, 158, 39-55. doi:10.1016/j.future.2024.02.009.