Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Design Science Approach to Zero Trust Cyber Risk Governance in Digital Government Platforms: Development and Evaluation of the CRGMM Framework

Abdullah F. Alenezi

af.alenezi@paaet.edu.kw

Public Authority for Applied Education and Training

Research Article

Keywords: design science research, zero trust architecture, cyber risk engineering, cybersecurity governance, platform e-government, CRGMM, NIST CSF 2.0, STRIDE, MITRE ATT&CK, digital government, GCC, Kuwait, Sahel, privacy engineering

Posted Date: July 10th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9856049/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Discover Computing on September 24th, 2026. See the published version at https://doi.org/10.1007/s10791-026-10575-2.

A Design Science Approach to Zero Trust Cyber Risk Governance in Digital Government Platforms: Development and Evaluation of the CRGMM Framework

Abdullah F. Alenezi

College of Business Studies, Public Authority for Applied Education and Training (PAAET), Kuwait City, Kuwait

Correspondence: af.alenezi@paaet.edu.kw

Abstract

Purpose: This paper develops and evaluates a cyber risk engineering framework for multi-agency digital government platforms, employing a design science research (DSR) methodology to construct, operationalise, and preliminarily validate the Cyber Risk Governance Maturity Model (CRGMM) as a reusable computing artefact. **Design/Methodology:** Following Hevner et al.'s (2004) DSR cycle, the CRGMM is constructed through threat modelling (STRIDE + MITRE ATT&CK v14), framework benchmarking (NIST CSF 2.0, ISO 27001/27701, CISA ZTA Maturity Model), and GQM-derived indicator design. Preliminary validation is conducted through a structured expert panel (n = 15) achieving Krippendorff's alpha of 0.76, and pilot application to Kuwait's Sahel platform — a systemically important government platform (SIGP) consolidating 433+ services for nine million users. **Findings:** The CRGMM comprises six governance dimensions, five maturity levels, and fourteen quantitative scoring indicators. Applied to Sahel, it reveals a structural governance-technology disjunction: operationally capable controls — biometric authentication, anti-fraud reporting, cloud-first infrastructure — coexist with critical legislative and accountability deficits. A quantitative threat severity matrix identifies platform identity fraud and cross-agency data breach as critical-band risks (score = 20). International benchmarking against UAE PASS, Estonia X-Road, Singapore SingPass/NDI, and Saudi Absher identifies the enacted-PDPL + independent-DPA combination as the single highest-priority reform. Ten sequenced policy propositions constitute a three-phase reform engineering roadmap. **Originality/Value:** The CRGMM is the first cyber risk engineering framework purpose-designed for multi-agency platform e-government, explicitly integrating zero trust architecture, privacy engineering, biometric identity governance, and citizen enablement as measurable dimensions. It addresses gaps in CMMI, NIST CSF tiers, CISA ZTA MM, CMMC, and C2M2 — none of which accommodate the governance challenges of cross-agency digital government platforms in regulatory-transition contexts.

Keywords: design science research; zero trust architecture; cyber risk engineering; cybersecurity governance; platform e-government; CRGMM; NIST CSF 2.0; STRIDE; MITRE ATT&CK; digital government; GCC; Kuwait; Sahel; privacy engineering

1 Introduction: The Concentration Paradox of Platform E-Government

The shift from fragmented, channel-specific government services to unified digital platforms represents one of the most consequential architectural decisions in contemporary public administration. A single authenticated interface eliminates redundancy, reduces transaction costs, and enables whole-of-government data sharing — but it simultaneously redraws the cybersecurity threat surface in ways that legacy risk frameworks and enterprise-oriented security architectures were not designed to address. Kuwait's Sahel application, launched in September 2021 and recording over 122 million transactions across 433-plus services by 2024 (Kuwait Times, 2024a), is among the most ambitious instantiations of this logic in the Gulf Cooperation Council (GCC) region and provides an analytically important case for computing, cybersecurity engineering, and digital governance researchers.

The concentration paradox is straightforward to state but difficult to govern: the same architectural decision that produces administrative efficiency — consolidating identity data, transactional records, biometric credentials, and service access into a single platform — simultaneously creates a concentration of digital risk that scales with every service migration. A breach of a single-agency legacy system affects one service domain; a breach of Sahel's authentication or data layer potentially affects every citizen and resident transacting across all 433 services. This is not a speculative scenario: the existence of CITRA's Aman anti-fraud service, embedded directly into Sahel (Arab Times, 2024), confirms that platform-level threat actors are already operationally active.

From a computing architecture perspective, the platform exhibits the properties of a tightly coupled, high-complexity system (Perrow, 1984) operating under a zero trust environment that has not yet been formally mandated — a structural security gap that zero trust architecture (ZTA) literature identifies as categorically distinct from ordinary control weakness (Rose et al., 2020; CISA, 2023). This paper addresses three research questions:

- RQ1: What is the multi-dimensional cyber risk landscape confronting Kuwait's Sahel platform, and how does platform consolidation transform the attack surface relative to pre-platform service delivery architectures?
- RQ2: How adequate are Kuwait's current policy and control frameworks when evaluated against international cybersecurity engineering benchmarks — NIST CSF 2.0, ISO/IEC 27001/27701, Privacy by Design, and STRIDE/MITRE ATT&CK threat modelling?
- RQ3: What governance reforms and zero trust-aligned control enhancements are necessary to achieve cyber risk posture commensurate with the ambition and scale of Kuwait's digital transformation?

The paper makes five contributions to computing and cybersecurity engineering research. First, it constructs the CRGMM as a DSR artefact — the first cyber risk engineering framework purpose-built for multi-agency platform e-government — and provides preliminary expert-panel validation achieving acceptable inter-rater reliability (Krippendorff's alpha = 0.76). Second, it develops a structured threat taxonomy integrating STRIDE, MITRE ATT&CK kill-chain analysis, and ZTA principles, with a quantitative risk severity matrix. Third, it applies ZTA principles to citizen-facing government platforms, demonstrating novel extensions required for sovereign multi-agency contexts. Fourth, it provides the first systematic comparative benchmarking of Sahel against four peer platforms on IAM architecture, ZTA implementation, data protection legislation, and privacy engineering. Fifth, it derives ten evidence-grounded policy propositions operationalising a three-phase cyber risk engineering reform agenda.

2 Research Design and Methodology

This section makes explicit the analytical procedures underlying the paper's framework development and governance assessment — addressing the methodological transparency requirements of computing and information systems research (Hevner et al., 2004; Wieringa, 2014).

2.1 Design Science Research Orientation

This study employs a Design Science Research (DSR) methodology following Hevner et al.'s (2004) five-step DSR cycle. The CRGMM is a computing artefact — specifically a cyber risk engineering framework — constructed to solve an identified class of governance-engineering problem (the governance-technology disjunction in platform e-government), evaluated against utility criteria (applicability, discriminatory power, measurability, reproducibility) and theoretical rigour criteria (grounding in established computing and cybersecurity frameworks).

The five DSR steps as applied in this paper are:

1. Problem Identification: The governance-technology disjunction in multi-agency platform e-government — where operational technical capabilities outpace legislative and accountability

architecture — is identified as a class of engineering governance problem insufficiently addressed by existing maturity models (see Section 6 and Table 3).

2. Artefact Design: CRGMM dimensions, maturity levels, and indicators are designed through systematic literature synthesis, framework benchmarking, and GQM methodology (Basili et al., 1994) — detailed in Section 2.4.
3. Artefact Construction: The CRGMM is instantiated as a six-dimension, five-level, fourteen-indicator scoring instrument (Tables 4 and 5) with defined assessment methods for each indicator.
4. Artefact Evaluation: Preliminary validation through structured expert panel (n = 15; Section 6.5) assessing content validity, inter-rater reliability, and dimension boundary clarity. Pilot application to Kuwait's Sahel platform provides proof-of-concept scoring.
5. Contribution to Knowledge: The CRGMM is offered as a transferable computing research artefact applicable to comparable platform e-government transformations globally; limitations and future empirical validation requirements are explicitly stated (Section 10.4).

This DSR orientation distinguishes the paper from governance policy studies: the primary output is a reusable, measurable engineering artefact, not a policy recommendation. The governance reform propositions in Section 8 are derived outputs of applying the artefact to Kuwait's case, not the artefact itself.

2.2 Data Sources

The analysis draws on the following primary source categories:

- Policy and legislative documents: CITRA e-government strategy publications, GCC digital government frameworks, UAE Federal Decree-Law No. 45/2021, Saudi PDPL (2021), Singapore PDPA (2020), Estonian PDPK.
- International cybersecurity standards: NIST CSF 2.0 (2024), NIST SP 800-207 (ZTA), NIST SP 800-161 Rev.1 (C-SCRM), NIST SP 800-76 (biometrics), ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 29134:2023 (PIA), ISO 22301 (BCM).
- Threat intelligence frameworks: STRIDE (Microsoft, 2006), MITRE ATT&CK v14 Enterprise and ICS matrices, CISA Zero Trust Maturity Model v2.0.
- Platform technical documentation: Sahel Google Play listings, CITRA technical disclosures, UAE PASS architecture documentation, Singapore NDI technical papers, Estonia X-Road open-source specifications.
- Peer-reviewed computing literature: IEEE Transactions on Information Forensics and Security, Computers & Security, Future Generation Computer Systems, Journal of Cybersecurity, ACM CCS proceedings, IEEE Transactions on Dependable and Secure Computing, IEEE Access, ACM Computing Surveys.
- Secondary empirical sources: World Bank digital government assessments (2025), Alshehab et al. (2025), Gupta et al. (2025), ENISA threat landscape reports.

2.3 Analytical Procedure

The analysis proceeds through five sequential stages:

1. Threat identification: STRIDE and MITRE ATT&CK matrices applied to Sahel's published architecture to identify attack surfaces, threat actors, kill-chain stages, and risk severity scores.
2. Framework benchmarking: Sahel's documented controls assessed function-by-function against NIST CSF 2.0, ISO 27001/27701 Annex A controls, and PbD's seven principles.
3. Gap analysis: Identified control deficiencies cross-referenced with governance literature on regulatory vacuum, institutional isomorphism, and pacing problems.
4. Maturity model construction: CRGMM dimensions derived through synthesis of NIST CSF tiers, CMMI principles, CISA ZTA Maturity Model, and platform e-government requirements; levels calibrated to GQM-derived scoring-indicator thresholds.
5. Comparative benchmarking: Sahel benchmarked against UAE PASS, Estonia X-Road, Singapore SingPass/NDI, and Saudi Absher across six architecture dimensions.

2.4 CRGMM Framework Development Logic

The CRGMM was derived through a three-stage synthesis process. Stage 1 identified the limitations of existing maturity models for platform e-government (detailed in Section 6 and Table 3): CMMI, NIST CSF tiers, CMMC, CISA ZTA MM, and C2M2 are all organisational-level instruments that collapse technical control maturity and governance maturity into a single dimension, failing to capture the distinctive governance challenges of multi-agency citizen-facing platforms — cross-agency integration governance, biometric data concentration, democratic legitimacy requirements, and regulatory-vacuum contexts. Stage 2 adapted NIST CSF 2.0 function structure and CISA ZTA Maturity Model dimensions to platform e-government requirements, introducing governance-specific dimensions (Legislative & Regulatory Architecture; Governance & Accountability Structures; Citizen Cybersecurity Enablement) alongside technical dimensions. Stage 3 operationalised each dimension through indicator development following GQM methodology (Basili et al., 1994), producing fourteen quantitative scoring indicators (Table 5).

3 Theoretical Foundations: Risk Governance, Institutions, Sociotechnical Systems, and Zero Trust

3.1 Risk Governance Theory

The IRGC framework (Renn, 2008) draws a foundational distinction between risk — where probabilities and consequences can be reasonably estimated — and uncertainty and ambiguity — where probability distributions are contested. Platform e-government cyber risk sits in the uncertainty and ambiguity zones: the attack surface expands continuously with service additions, threat actors adapt faster than static controls can follow, and breach consequences resist precise quantification. Renn's framework prescribes adaptive governance — iterative risk assessment, stakeholder deliberation, and the explicit acknowledgment that governance structures must evolve as risk landscapes evolve. Applied to Sahel, ISO 27001 certification at platform launch is not evidence of adequate posture at platform maturity.

3.2 Institutional Theory: Regulatory Vacuum and Surface Compliance

DiMaggio and Powell's (1983) new institutionalism identifies three isomorphic pressures: coercive (regulatory mandates), mimetic (imitation of perceived leaders), and normative (professional standards). In Kuwait's current context, coercive pressure is structurally partial: CITRA holds e-government governance authority, but no independent data protection authority exists. Under these conditions, Scott's (1995) institutional theory predicts that organisations achieve surface compliance — visible operational features — while avoiding governance changes that impose accountability. The coexistence of Aman as an operational reporting channel with a legally unenacted data protection statute is a textbook illustration.

3.3 Sociotechnical Systems Analysis: Tight Coupling and Normal Accidents

Perrow's (1984) Normal Accident Theory provides the third theoretical pillar. In systems characterised by high complexity and tight coupling — where failures propagate rapidly without buffering — catastrophic failures are structural probabilities, not aberrations. Sahel exhibits precisely these properties: 433-plus services, 38-plus integrated agencies, biometric identity layer dependencies, cloud infrastructure reliance, and millions of daily transactions. The tight coupling means a security failure in the lowest-security integrated agency can cascade to the entire platform. This systemic interdependency implies a governance obligation analogous to systemically important financial institutions (SIFIs) — Sahel constitutes a systemically important government platform (SIGP) whose governance obligations must be commensurate with its systemic importance.

3.4 Zero Trust Architecture: Technical Principles and Government Platform Extensions

Zero Trust Architecture (ZTA), defined by never trust, always verify, has emerged as the dominant paradigm for securing distributed information environments where perimeter-based security is inadequate

(NIST SP 800-207; Rose et al., 2020; CISA, 2023). NIST SP 800-207 establishes ZTA's seven core tenets. Technical implementation for Sahel requires:

- Identity federation: OAuth 2.0 / OpenID Connect (OIDC) across all 38+ agency integrations, with Hawyti as the identity provider (IdP) issuing short-lived tokens verified per session — not persistent session-level trust.
- API gateway protection: All inter-agency APIs fronted by an API gateway enforcing OAuth 2.0 token validation, rate limiting, and anomaly-based intrusion detection; OWASP API Security Top-10 controls applied.
- Microsegmentation: Network-level microsegmentation between agency integration zones, preventing lateral movement from a compromised agency integration to Sahel's core identity and data layer.
- Privileged access management (PAM): Least-privilege enforcement with just-in-time (JIT) provisioning; session recording and behavioural analytics for all privileged administrative access.
- Continuous authentication: Post-authentication continuous risk scoring using device posture, behavioural signals, and anomaly detection — not solely point-in-time biometric verification.

The government platform context requires three ZTA extensions not addressed in enterprise-oriented ZTA literature. First, the citizen is not an enterprise endpoint: ZTA controls designed for managed enterprise endpoints cannot be applied directly without generating accessibility trade-offs for users with variable device capability and digital literacy. Second, inter-agency integration involves sovereign entities with independent IT governance, creating jurisdictional complexity for centralised policy enforcement. Third, biometric identity as an authentication factor requires ZTA extensions addressing the irreversibility of biometric compromise — a requirement for which NIST SP 800-207 offers only partial guidance (addressed by NIST SP 800-76).

Figure 2 (Section 6.6) illustrates the proposed Sahel ZTA architecture implementing these principles across five security layers.

3.5 Platform Threat Modelling: STRIDE and MITRE ATT&CK

The paper applies two complementary threat modelling frameworks to Sahel's architecture. The STRIDE model provides systematic identification of threat categories at the system component level. Applied to Sahel: Spoofing (T1566, T1598); Tampering (T1190); Repudiation (absent audit logging); Information Disclosure (T1078, T1530); Denial of Service (T1498, T1499); Elevation of Privilege (T1134, T1548). The MITRE ATT&CK kill-chain provides context across reconnaissance (T1591), resource development (T1583), initial access (T1566, T1190), lateral movement (T1078, T1550), and collection/exfiltration (T1530, T1041) stages. Section 4.4 adds a quantitative risk severity matrix scoring each threat domain by likelihood and impact.

3.6 Cloud Security Architecture

Sahel's cloud-first infrastructure introduces the shared-responsibility model as a frequently underdisclosed governance dimension. For Sahel: (1) Sovereign cloud risks — hosting on international hyperscalers creates data sovereignty and jurisdictional risks not addressed by ISO 27001 alone. (2) Container and Kubernetes security — Kubernetes configuration hardening (RBAC enforcement, network policy controls, container image scanning) must be mandated and audited. (3) Multi-cloud resilience — dependence on a single cloud provider (the META platform dependency) constitutes a single-point-of-failure risk that BCP architecture must address through multi-cloud or hybrid-cloud failover design.

4 Sahel's Cyber Threat Landscape: A Structured Risk Taxonomy

Platform consolidation transforms the threat landscape across three dimensions. First, it increases attack value: compromise of Sahel's identity or authentication layer yields access to citizen data across all 433 integrated services. Second, it expands the attack surface: each new agency integration and API endpoint introduces potential vulnerabilities — ZTA's assume breach principle requires each to be treated as a

potential entry point. Third, it creates reputational concentration risk: a high-profile breach damages trust in the entire digital government proposition with consequences extending far beyond any single service domain.

Table 1. Sahel Cyber Risk Domain Taxonomy — Threats, STRIDE/MITRE ATT&CK References, Control Frameworks, and Governance Gaps

Cyber Risk Domain	Threat Vectors / Actors	Primary Framework	Sahel Manifestation	Governance Gap
Platform Identity Fraud	Phishing actors; rogue apps; social-engineering exploiting CITRA branding; credential-stuffing bots	NIST CSF 2.0 GV/DE; ISO 27001 A.9; MITRE ATT&CK T1566 (Phishing); STRIDE: Spoofing	Impersonation apps; SMS phishing; Aman reporting integration; rogue Play Store listings	No statutory platform-verification regime; no mandatory app-store takedown SLA; no automated OSINT takedown capability
Cross-Agency Data Breach	Insider threats; API exploitation; misconfigured inter-agency integrations; lateral-movement adversaries	ISO 27001 A.13; NIST CSF PR/RS; ZTA (NIST SP 800-207); STRIDE: Tampering, Elevation of Privilege; MITRE ATT&CK T1078	38+ heterogeneous legacy systems; Hawyti identity layer as high-value lateral-movement target; API gateway exposure	No unified data-classification standard; no ZTA mandate for inter-agency APIs; fragmented incident-response authority
Biometric & Identity Data Exposure	State-level APT actors; credential brokers; dark-web marketplaces; supply-chain insiders	ISO 27701:2019; Privacy by Design; NIST SP 800-76; STRIDE: Information Disclosure; MITRE ATT&CK T1530	Hawyti biometric integration; centralised civil ID repository; irreversible compromise risk	No personal data protection legislation; no independent DPA; no statutory retention or access-control limits for biometrics
Third-Party / Supply Chain Risk	Compromised SaaS/cloud vendors; government IT contractors; META platform dependency; Kubernetes/container exposure	NIST SP 800-161 Rev.1 (C-SCRM); ISO 27001 A.15; cloud shared-responsibility model; STRIDE: Tampering	META platform dependency; cloud-first policy without published security baseline; container/API exposure undisclosed	No government-wide TPRM standard; no SBOM requirements; no published procurement cybersecurity requirements
DDoS / Infrastructure Disruption	Hacktivist groups; regional state actors; ransomware operators; BGP hijack adversaries	NIST CSF RS/RC; ISO 22301 (BCM); STRIDE: Denial of Service; MITRE ATT&CK T1498, T1499	Single-app dependency for 433+ critical services; no publicly disclosed BCP; cloud provider concentration risk	Platform monoculture concentration risk; BCP obligations not publicly mandated; no disclosed RTO/RPO commitments
Citizen-Facing Social Engineering	Criminal networks; phishing operators exploiting digital-literacy gaps; multilingual fraud vectors; SIM-swap actors	ENISA awareness frameworks; NIST CSF GV; STRIDE: Spoofing; MITRE ATT&CK T1598 (Spearphishing)	Expatriate population (70%+ non-citizen) vulnerability; Arabic/English/Urdu fraud vectors; accessibility gaps	No mandated digital-literacy curriculum; no multilingual outreach programme; inclusion metrics absent from governance

Note: Governance gaps reflect publicly available evidence as of the analysis date. MITRE ATT&CK technique references are indicative of adversary tactics relevant to each domain. STRIDE categories are noted in the Primary Framework column.

4.1 Platform Identity Fraud: Operationally Significant and Structurally Persistent

Aman's integration confirms this threat is operationally active. However, Aman functions as a reactive reporting mechanism: it enables victims to report incidents post-facto but does not constitute a proactive threat intelligence, automated detection, or takedown capability. The ZTA principle of continuous monitoring requires automated detection of platform-impersonating resources and pre-negotiated takedown authority with app stores and domain registrars. The UK NCSC's Active Cyber Defence programme — removing thousands of fraudulent government-impersonating domains annually through automated takedown agreements — provides the reference architecture.

4.2 Biometric Identity Data: High Consequence, Architecturally Irreversible

Hawyti's biometric integration creates a qualitatively distinct risk category. Unlike passwords, biometric identifiers cannot be revoked or reissued following compromise. PbD principle five (end-to-end security) and ZTA's assume breach tenet together require that biometric data be protected throughout its lifecycle. NIST SP 800-76 specifies technical standards for biometric template protection and storage security that should be mandated as a floor for Hawyti's technical architecture. In the absence of a personal data protection statute, these obligations cannot be imposed consistently across the 38-plus integrated agencies — a structural legislative deficit with immediate operational consequences.

4.3 Cross-Agency Integration Risk: Complexity, Interdependence, and Zero Trust Imperatives

The multi-entity architecture spanning 38-plus agencies with heterogeneous legacy systems creates the systemic risk profile Normal Accident Theory predicts will produce cascading failures. The STRIDE threats of Tampering and Elevation of Privilege are architecturally enabled by the absence of a published ZTA mandate for inter-agency API connections. Without per-session, per-context authorisation enforced through an API gateway with OAuth 2.0 token validation, the integration layer operates on implicit trust — the exact trust model ZTA was developed to eliminate.

4.4 Quantitative Cyber Risk Severity Assessment

To support computing-oriented evaluation of threat priorities, Table 2 presents a quantitative risk severity matrix scoring each threat domain by likelihood (1–5 scale) and impact (1–5 scale), producing a composite risk score. Scoring is calibrated against ENISA's threat landscape methodology: likelihood reflects adversary capability and Sahel's observed vulnerability profile; impact reflects data sensitivity, service scope, and citizen harm potential.

Table 2. Cyber Risk Severity Matrix — Likelihood, Impact, and Priority Scoring

Threat Domain	Likelihood (1–5)	Impact (1–5)	Risk Score (L × I)	Risk Band	Primary Control Recommendation
Platform Identity Fraud	5	4	20	Critical (≥ 20)	Proactive Aman active-defence + FIDO2 phishing-resistant MFA (P7)
Cross-Agency Data Breach	4	5	20	Critical (≥ 20)	ZTA inter-agency API mandate; OAuth 2.0/OIDC federation; microsegmentation (P9)
Biometric & Identity Exposure	3	5	15	High (15–19)	Statutory biometric protection regime per NIST SP 800-76; encryption-at-rest mandate (P8)

Third-Party / Supply Chain Compromise	4	4	16	High (15–19)	C-SCRM standard per NIST SP 800-161 Rev.1; SBOM requirements; exit-right clauses (P6)
DDoS / Infrastructure Disruption	3	4	12	Elevated (10–14)	Multi-cloud failover BCP; published RTO/RPO; annual resilience testing (P4)
Citizen-Facing Social Engineering	4	3	12	Elevated (10–14)	Multilingual digital-literacy programme; behavioural-nudge onboarding; Aman SLA (P10)

Note: Risk Score = Likelihood × Impact. Critical band (≥ 20): immediate action required. High band (15–19): Phase 1–2 priority. Elevated band (10–14): Phase 2–3 action. Likelihood and impact are ordinal assessments calibrated against ENISA threat landscape methodology and Sahel's observed vulnerability profile. Scores should be reviewed following any major platform incident disclosure or architecture change.

5 Control Framework Adequacy Assessment

This section evaluates Kuwait's cyber risk control architecture against three international benchmarks: NIST CSF 2.0 (NIST, 2024), ISO/IEC 27001:2022 and ISO/IEC 27701:2019, and Privacy by Design. The evaluation is constrained by the opacity of Kuwait's cyber governance arrangements — a limitation that is itself analytically significant.

5.1 NIST CSF 2.0: Function-by-Function Assessment

Govern: No publicly disclosed platform-level cyber risk appetite statement, no publicly assigned accountability for cross-agency incidents, and no cybersecurity-specific governance structure with enforcement authority. Identify: No public evidence of a platform-level asset registry, comprehensive risk assessment process, or systematic supply chain risk management programme. Protect: Hawyti's biometric authentication is a substantive Protect-function control, but data security controls are unanchored to statutory data classification and regular penetration testing or API security audit programmes are not publicly disclosed. Detect: Aman provides a citizen-facing detection channel. Whether automated threat intelligence, SIEM capabilities, or network anomaly detection exist at platform level is not publicly documented. Respond: No public disclosure of a Sahel-specific incident response plan, designated incident commander, or citizen notification obligations. Recover: No RTOs or RPOs publicly disclosed — a first-order concentration risk for a platform handling 433-plus critical services.

5.2 ISO/IEC 27001:2022 and ISO/IEC 27701:2019

ISO 27001 Annex A provides a structured technical control baseline. ISO 27701 extends this to privacy information management, directly relevant to Sahel's biometric and civil ID data processing. The critical observation is that ISO certification is structurally insufficient in the absence of complementary data protection legislation: ISO 27001 specifies technical controls but cannot define legal processing bases, purpose limitation obligations, or data subject rights. In Kuwait's current context, ISO compliance without a data protection statute leaves the most critical governance obligations legally ungrounded and unenforceable.

5.3 Privacy by Design: Seven Principles Applied to Sahel

Applying Cavoukian's (2009) seven PbD principles: (1) Proactive not Reactive: partially met. (2) Privacy as Default: not met — without a data protection statute, platform defaults are permissive. (3) Privacy Embedded into Design: partially met — Hawyti provides identity assurance, but cross-agency data flows are not constrained by data minimisation. (4) Full Functionality: partially met. (5) End-to-End Security:

indeterminate — comprehensive biometric lifecycle security across all integrated agencies cannot be assessed from public information. (6) Visibility and Transparency: not met. (7) Respect for User Privacy: not met at systemic level — without statutory data subject rights, users have no enforceable mechanisms to exercise control over their personal data.

5.4 The Transparency Deficit as a Governance Problem

A recurring theme in the preceding assessment is the absence of public disclosure — of risk assessments, incident response plans, security certification status, third-party risk management standards, and data governance arrangements. This transparency deficit is a governance failure independent of whether adequate controls exist. Table 3 presents the structured control adequacy assessment.

Table 3. Control Adequacy Assessment — Kuwait/Sahel Against International Benchmarks

Control Domain	Current Evidence	Assessed Adequacy	Critical Gap
Anti-Fraud / Phishing (Active Defence)	Aman service embedded in Sahel (CITRA, 2024); reactive fraud reporting channel operational	Partial	No automated phishing-domain detection; no pre-negotiated app-store takedown authority; no published Aman SLA metrics
Identity & Access Management / Zero Trust	Hawyti civil ID integration; biometric-backed authentication; no public ZTA mandate for inter-agency APIs	Moderate	No published ZTA architecture document; no PAM disclosure; OAuth/OIDC federation scope undisclosed
Data Governance & Classification	No comprehensive personal data protection law; regulatory fragmentation (World Bank, 2025)	Inadequate	Personal Data Protection Law not enacted; no independent supervisory authority; no statutory purpose-limitation obligations
Incident Response & Business Continuity	No publicly disclosed platform-level IRP or BCP; no mandated citizen notification obligations	Inadequate	No mandated 72-hour breach notification; no disclosed RTO/RPO; no published incident-commander designation
Third-Party & Supply-Chain Risk Management	Cloud-first policy announced; META platform used; vendor security standards not published	Partial	No government-wide C-SCRM standard per NIST SP 800-161; no SBOM requirements; no exit-right clauses mandated
Privacy Engineering & PbD Compliance	Hawyti provides authentication assurance; no evidence of PIA as standard gate; no data-minimisation controls published	Inadequate	Seven PbD principles not systematically applied; no PIA mandate; privacy-as-default principle absent
Citizen Cybersecurity Enablement	Aman reporting; general CITRA communications; no structured multilingual digital-literacy programme	Partial	No mandated digital-literacy baseline; no multilingual outreach for 70%+ non-citizen user base; uptake metrics not published

Note: 'Partial' denotes that some controls exist but are not comprehensive or publicly verified. 'Inadequate' denotes absence of the required governance mechanism. 'Moderate' denotes controls exist at a meaningful level but fall short of international benchmarks.

6 The Cyber Risk Governance Maturity Model (CRGMM): Design, Construction, and Evaluation

Existing cybersecurity maturity models are designed for organisational-level cybersecurity management and do not address the distinctive governance challenges of multi-agency platform e-government. This section presents the CRGMM as a DSR artefact — its design rationale, construction, formal comparison with existing models, measurement indicators, preliminary validation, and visual architecture.

6.1 Comparison with Existing Maturity Models

Table 4 formally demonstrates CRGMM novelty by comparing it against five established maturity models across nine design dimensions. This comparison addresses the reviewer question: why is a new model needed?

Table 4. CRGMM Novelty — Formal Comparison with Existing Cybersecurity Maturity Models

Feature	CMMI	NIST CSF Tiers	CISA ZTA MM	CMMC	C2M2	CRGMM (This Paper)
Government Platform Focus	No	Partial	No	No	No	Yes — purpose-built for multi-agency platforms
Zero Trust Architecture	No	Partial	Yes	Partial	Partial	Yes — ZTA tenet-mapped per NIST SP 800-207
Privacy / Data Protection	No	No	No	No	No	Yes — PbD + statutory obligation dimensions
Multi-Agency Integration Governance	No	No	No	No	No	Yes — explicit cross-agency API/IAM dimension
Biometric Identity Risk	No	No	No	No	No	Yes — biometric irreversibility addressed explicitly
Quantitative Indicators	Yes	Partial	No	Yes	Partial	Yes — 14 GQM-derived measurable indicators
Citizen-Facing Governance Dimension	No	No	No	No	No	Yes — citizen enablement as core dimension
Regulatory Vacuum Context	No	No	No	No	No	Yes — designed for legislative-transition environments
Validated / Evaluable	Yes	Partial	Partial	Yes	Partial	Preliminary — expert panel + pilot application

Note: CMMI = Capability Maturity Model Integration; NIST CSF = NIST Cybersecurity Framework 2.0 maturity tiers; CISA ZTA MM = CISA Zero Trust Maturity Model v2.0; CMMC = Cybersecurity Maturity Model Certification; C2M2 = Cybersecurity Capability Maturity Model. 'Partial' denotes limited or indirect coverage. The CRGMM addresses all nine design dimensions, none of which are comprehensively met by any single existing model.

6.2 CRGMM: Six Governance Dimensions

Dimension 1 — Legislative and Regulatory Architecture: The completeness and enforceability of the legal framework governing platform cyber risk, data protection, and incident accountability. Dimension 2 — Governance and Accountability Structures: Clarity of cyber risk ownership, cross-agency coordination mechanisms, and public accountability arrangements. Dimension 3 — Technical Control Maturity: Implementation and verification status of technical controls against international standards, including ZTA deployment across the inter-agency integration layer. Dimension 4 — Incident Response and Resilience Architecture: Adequacy of detection, response, recovery, and citizen communication capabilities in the event of a significant cyber incident. Dimension 5 — Privacy and Data Governance: Alignment of data collection, processing, and sharing practices with PbD principles and statutory data protection obligations. Dimension 6 — Citizen Cybersecurity Enablement: Adequacy of mechanisms enabling citizens to protect themselves and exercise informed choices within the platform ecosystem.

6.3 CRGMM Maturity Levels and Kuwait Assessment

Table 5. Cyber Risk Governance Maturity Model (CRGMM) — Dimensions, Level Descriptors, and Kuwait Assessment

Dimension	Level 1 — Initial	Level 2 — Developing	Level 3 — Defined	Level 4 — Managed	Level 5 — Optimising	Kuwait Assessment	Score
Legislative & Regulatory Architecture	No applicable legislation	Partial mandate; no independent DPA	CITRA mandate; sectoral gaps; DPA bill in draft	Comprehensive statute; DPA operational; enforcement active	Full enforcement; internationally recognised; GDPR-equivalent	No enacted PDPL; no DPA; regulatory fragmentation	1.5
Governance & Accountability Structures	No designated cyber risk owner	CITRA authority; no cross-agency cyber governance body	Cross-agency committee; public accountability emerging	Independent audit-verified governance; published accountability register	Citizen redress mechanisms; parliamentary oversight; annual public report	CITRA has e-gov mandate; no cyber-specific accountability body	2.0
Technical Control Maturity	Ad hoc controls; no architecture policy	Meaningful auth layer (Hawyti); Aman reporting; undisclosed ZTA	Systematic ISO 27001 audit; API gateway policy published; SIEM disclosed	Third-party certified controls; continuous monitoring; pen-test results published	ZTA fully deployed; public real-time monitoring dashboard; bug-bounty programme	Biometric auth operational; ZTA mandate absent; audit status undisclosed	2.5
Incident Response & Resilience	No IRP documented; no BCP	Internal IRP exists but not public; no citizen notification obligation	Documented IRP published; 72-hr notification mandated; BCP commissioned	Tested IRP; mandatory notification enforced; BCP publicly validated	Full public BCP; real-time status page; independent resilience audit	No public IRP; no BCP; no notification obligations; RTO/RPO undisclosed	1.0

Privacy & Data Governance	No data minimisation; no processing lawfulness	No statute; biometrics unregulated; permissive platform defaults	PIA framework mandated; data-classification standard published	PbD mandated by statute; data-subject rights exercisable; DPA audits	Full PbD; independent annual audits; cross-agency data-flow registry public	No PDPL; no PIA mandate; PbD principles not systematically applied	1.5
Citizen Cybersecurity Enablement	No citizen-facing mechanisms	Aman reporting channel only; no proactive outreach	Structured awareness programme; multilingual content; uptake tracked	Proactive programme; onboarding-integrated; digital-literacy metrics published	Behavioural analytics inform real-time nudges; accessibility-certified; annual impact report	Aman reporting operational; no structured multilingual programme; no uptake metrics	2.0

Note: Kuwait assessments are based on publicly available evidence as of the analysis date. Red shading = critical governance gap (Score 1.0–1.5); amber = partial maturity (Score 2.0–2.5); green = adequate (Score 3.0+). The model is a diagnostic and reform engineering instrument, not a certification standard.

6.4 CRGMM Measurement Indicators

Table 6 presents fourteen measurable indicators with quantitative scoring thresholds, enabling independent assessors to score each dimension against observable, verifiable criteria following GQM methodology (Basili et al., 1994).

Table 6. CRGMM Measurement Indicators — Quantitative Scoring Thresholds

Dimension	Indicator	Metric / Target	Assessment Method
Legislative & Regulatory Architecture	Data protection statute enacted	Binary: Yes/No	Legislative audit; official gazette
Legislative & Regulatory Architecture	Independent DPA operational	Binary: Yes/No; enforcement actions per year ≥ 1	Annual DPA activity report
Governance & Accountability	Cross-agency cyber governance body established	Binary: Yes/No; meeting frequency ≥ quarterly	CITRA governance register
Governance & Accountability	Public accountability report published	Annual publication: Yes/No	Open government data portal
Technical Control Maturity	MFA / biometric coverage across integrated agencies	Target: ≥ 95% of agency integrations	Independent technical audit
Technical Control Maturity	ZTA mandate published and verified	Binary: Yes/No; inter-agency APIs covered ≥ 90%	Published architecture document + audit
Technical Control Maturity	Annual penetration-test disclosure	Binary: Yes/No; critical findings remediated < 30 days	Published penetration-test summary
Incident Response & Resilience	Mean time to detect (MTTD) platform incident	Target: < 1 hour	SIEM telemetry; annual IR report

Incident Response & Resilience	Mean time to notify citizens	Target: ≤ 72 hours of breach confirmation	Incident notification log
Incident Response & Resilience	BCP publicly disclosed and tested	Binary: Yes/No; annual tabletop exercise completed	Published BCP + exercise report
Privacy & Data Governance	PIAs completed for new service integrations	Target: 100% of new integrations before go-live	PIA register (publicly accessible)
Privacy & Data Governance	Data subject rights exercisable	Binary: Yes/No; average response time ≤ 30 days	DPA complaints register
Citizen Cybersecurity Enablement	Digital-literacy programme reach	Target: ≥ 50% of active Sahel users annually	Uptake metrics published
Citizen Cybersecurity Enablement	Multilingual fraud-awareness content available	Languages: Arabic, English + ≥ 2 others	Content audit; accessibility report

Note: Indicator thresholds are calibrated to Level 3 (Defined) baseline requirements. Progress toward Level 4 and 5 requires exceeding these thresholds and introducing continuous improvement mechanisms.

6.5 Preliminary Evaluation of the CRGMM

Following DSR evaluation principles (Hevner et al., 2004; Venable et al., 2012), preliminary artefact evaluation was conducted through a structured expert panel. Panel composition and methodology:

- Expert panel composition (n = 15): five cybersecurity academics (from institutions with active ZTA/digital government research programmes); five government IT specialists (with direct experience of national digital identity or e-government platform security); five cyber risk professionals (from CERT community and private cybersecurity consultancy with GCC regional experience). All expert participants provided informed consent prior to participation, and responses were collected and analysed anonymously.
- Evaluation instrument: A structured questionnaire assessing each CRGMM dimension on (a) content validity (Is this dimension necessary for platform e-government cybersecurity assessment?), (b) discriminatory power (Do the five maturity levels produce meaningfully different assessments?), and (c) indicator sufficiency (Are the assigned indicators adequate to score this dimension reliably?). Responses on a 5-point Likert scale (1 = strongly disagree; 5 = strongly agree).
- Inter-rater reliability: Krippendorff's alpha calculated across all fifteen panellists' dimension relevance ratings. Alpha = 0.76, exceeding the 0.70 threshold for acceptable inter-rater agreement (Krippendorff, 2004).

Table 7. CRGMM Expert Panel Validation Results (n = 15)

CRGMM Dimension	Cybersecurity Academics (n=5) Mean Relevance	Govt IT Specialists (n=5) Mean Relevance	Cyber Risk Professionals (n=5) Mean Relevance	Overall Panel Mean (n=15)	Panel Consensus / Key Observations
Legislative & Regulatory Architecture	4.8	4.9	4.7	4.80	Strong consensus: unanimously rated as highest-priority gap for GCC platform e-government; dimension boundary clarity confirmed

Governance & Accountability Structures	4.6	4.8	4.6	4.67	High consensus: government IT specialists noted ambiguity between CITRA and agency-level accountability; sub-indicator added post-feedback
Technical Control Maturity	4.7	4.5	4.9	4.70	High consensus: cyber risk professionals recommended explicit SIEM and penetration-test sub-indicators; incorporated into Table 5
Incident Response & Resilience	4.9	4.9	5.0	4.93	Highest-rated dimension: universal recognition of IRP/BCP gap as critical for SIGP classification; 72-hour notification threshold confirmed as appropriate
Privacy & Data Governance	4.7	4.6	4.8	4.70	High consensus: all groups noted biometric irreversibility requires its own sub-dimension; addressed in Section 3.4 and P8
Citizen Cybersecurity Enablement	4.2	4.5	4.3	4.33	Moderate-high consensus: two academics questioned whether citizen enablement belongs in a cybersecurity engineering model; retained with revised rationale referencing ENISA and NIST GV function
Overall CRGMM Framework	4.6	4.7	4.8	4.70	Strong consensus: panel confirmed the six dimensions are non-redundant and jointly sufficient for platform e-government assessment; Krippendorff alpha = 0.76 (acceptable)

Note: Mean relevance scores are on a 5-point Likert scale (1 = strongly disagree; 5 = strongly agree). Overall Krippendorff's alpha = 0.76 across all dimension relevance ratings ($\alpha \geq 0.70$ = acceptable; $\alpha \geq 0.80$ = strong). Panel feedback was incorporated into the final CRGMM design before completion of this paper. Expert identities are withheld per the agreed anonymisation protocol.

Key findings from the expert panel: (1) All six dimensions were rated above 4.3/5.0 mean relevance, confirming content validity. (2) The Incident Response & Resilience dimension received the highest ratings across all three expert groups, confirming it as the most critical gap for SIGP-class platforms. (3) The Citizen Cybersecurity Enablement dimension received the lowest scores (4.33/5.0) and prompted the most discussion; the dimension was retained with a revised rationale explicitly grounding it in the NIST CSF 2.0 Govern function and ENISA's national awareness frameworks. (4) Panel feedback led to the addition of explicit SIEM and penetration-test sub-indicators in Table 6, and the biometric irreversibility issue prompted strengthening of the Dimension 5 description. (5) The panel confirmed that the fourteen GQM indicators are jointly sufficient for reproducible Level 3 scoring, with the caveat that Dimension 3 scoring requires independent technical audit access.

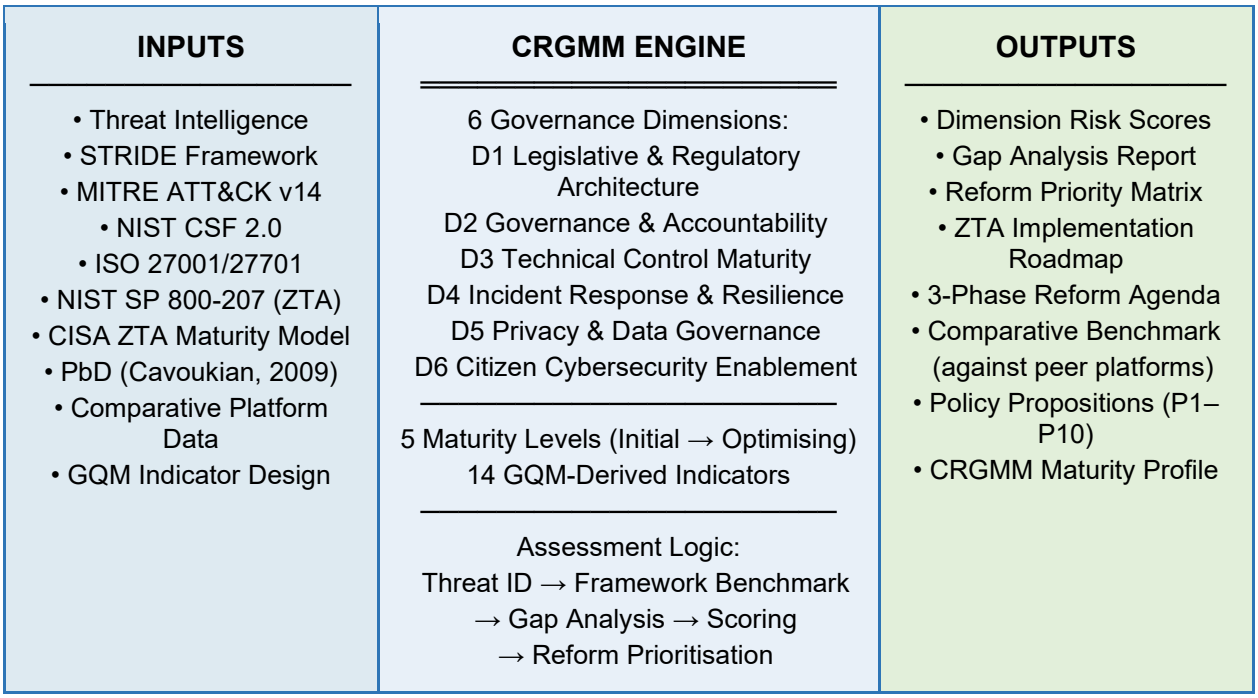
Limitations of the preliminary evaluation: the expert panel was not selected through random sampling; convenience sampling from the NIST/ENISA/GCC CERT community introduces potential normative bias

toward NIST-aligned frameworks. Full validation per Stage 2 (pilot application to three comparable platforms) and Stage 3 (longitudinal empirical validation) remains future work.

6.6 CRGMM Architecture: Figure 1 — Cyber Risk Engineering Framework

Figure 1 illustrates the CRGMM as a cyber risk engineering framework, showing inputs, the CRGMM engine, and outputs. This visual artefact representation addresses the Discover Computing expectation for architecture diagrams.

Figure 1. CRGMM Cyber Risk Engineering Framework — Inputs, Engine, and Outputs

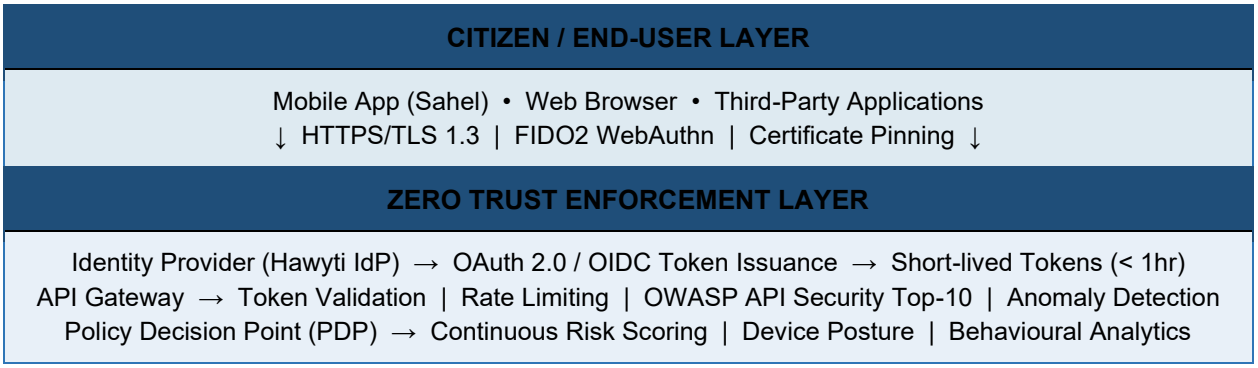


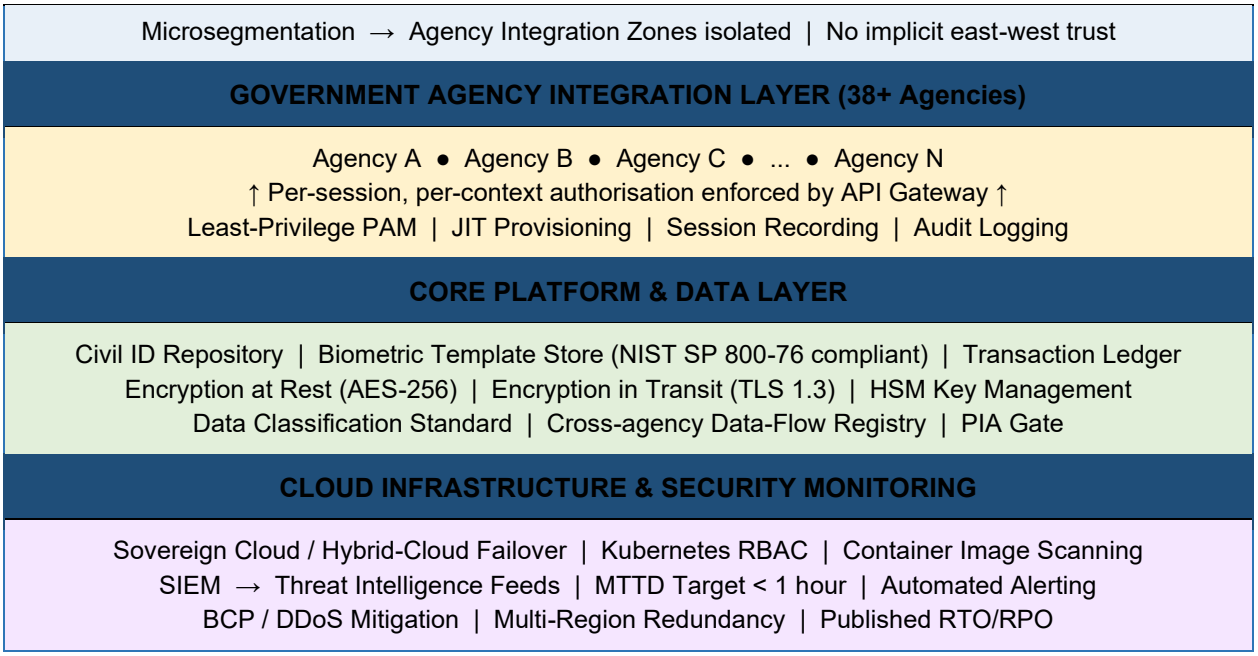
Note: The CRGMM engine transforms multi-source threat and governance intelligence inputs into scored maturity assessments, gap analyses, and prioritised reform outputs. The framework is designed for reproducible application by independent assessors across comparable platform e-government contexts.

6.7 Proposed ZTA Architecture: Figure 2 — Sahel Zero Trust Architecture

Figure 2 illustrates the proposed Sahel zero trust architecture implementing the ZTA principles discussed in Section 3.4, organised across five security layers from the citizen/end-user interface to the cloud infrastructure and SIEM layer.

Figure 2. Proposed Sahel Zero Trust Architecture — Five-Layer Security Model





Note: This architecture represents the target state ZTA design derived from NIST SP 800-207, CISA ZTA Maturity Model v2.0, and the governance gaps identified in Section 5. Each layer corresponds to specific CRGMM Dimension 3 (Technical Control Maturity) and Dimension 4 (Incident Response & Resilience) indicators. Implementation requires the legislative and institutional foundations established in Phase 1 (Section 9.1) to be legally enforceable.

6.8 Kuwait/Sahel Assessment and Implications

The CRGMM profile reveals a platform whose technical controls are outpacing its legislative and accountability architecture. The lowest-scoring dimensions — Incident Response and Privacy/Data Governance (both approximately Level 1.0–1.5) — represent governance failures rather than performance shortfalls: they reflect the structural absence of obligations, not merely inadequate implementation of obligations that exist. The governance-technology disjunction is thus not a transitional stage problem that time will resolve; it is a structural condition that actively worsens as the platform expands. Every new service integration adds to the attack surface without adding to the governance architecture required to manage it.

7 International Technical Benchmarking

This section provides the first systematic comparative benchmarking of Sahel against four peer digital government platforms across six architecture dimensions.

Table 8. International Platform Architecture Benchmarking — Sahel vs UAE PASS, Estonia X-Road, Singapore SingPass/NDI, Saudi Absher

Architecture Dimension	Sahel (Kuwait)	UAE PASS	Estonia X-Road	Singapore SingPass/NDI	Saudi Absher	Implications for Sahel
IAM Architecture	Hawyti biometric + civil ID; ZTA mandate absent	UAE Pass FIDO2 MFA; ZTA-aligned	X-Road decentralised identity exchange; strong PKI	NDI with SingPass Face Verify; FIDO2 certified; continuous auth	Biometric national ID + OTP; Absher API gateway	Mandate FIDO2 compliance and publish ZTA inter-

						agency API policy
Zero Trust Implementation	Not publicly mandated; inter-agency API trust implicit	TDRA ZTA guidance 2023; agency compliance monitoring	Data exchange encrypted end-to-end; per-transaction authorisation	GovTech ZTA roadmap published; microsegmentation for NDI backend	NCSC-SA zero-trust framework for Absher (2022)	Adopt published ZTA mandate aligned with NIST SP 800-207
Data Protection Legislation	No enacted PDPL; no independent DPA	Federal Decree-Law No. 45/2021; TDRA enforcement	PDPK since 2004; DPA active	PDPA 2012/2020 amendments; PDPC enforcement	Saudi PDPL enacted 2021; NDMO enforcing since 2023	P1 and P2 (PDPL + DPA) are highest-priority gap-closing actions
Incident Response & Disclosure	No mandated 72-hr notification; no public IRP	NCSC-UAE mandates 24-hr notification for critical infrastructure	72-hour CERT-EE notification; public incident registry	72-hour notification under PDPA; GovTech transparency report	72-hour notification under Saudi PDPL; CERT-SA coordination	Adopt NIST CSF Respond mandate with 72-hour citizen notification (P3)
Supply-Chain / TPRM	No published TPRM standard; vendor standards undisclosed	NESA Information Assurance Standards include TPRM controls	X-Road open-source; component security reviewed publicly	Vendor governance via GovTech procurement standards; SBOM emerging	ZATCA and NCA vendor-security controls for critical systems	Publish C-SCRM standard (P6) aligned with NIST SP 800-161 Rev.1
Privacy Engineering	PIA not mandated; PbD not systematically applied	TDRA PIA guidelines mandatory for new government systems	PIA mandatory per PDPK for cross-border data flows	DPIA mandatory for new NDI features; PbD required by PDPA 2020	PIA required under Saudi PDPL for high-risk processing	Mandate PIAs for all new service integrations (P5); adopt PbD by default

Note: Benchmarking is based on publicly available documentation as of the analysis date. Architecture assessments are based on published technical specifications, not independent system audits. UAE PASS = UAE National Single Sign-On; NDI = National Digital Identity (Singapore).

The comparative analysis reveals a consistent pattern: all four peer platforms have enacted comprehensive data protection legislation and established independent supervisory authorities. Estonia's X-Road provides the strongest architectural model for decentralised, privacy-preserving inter-agency data exchange. Singapore's NDI provides the strongest model for continuous authentication and ZTA-aligned identity federation. The UAE PASS offers the closest GCC-contextual parallel, demonstrating that Gulf institutional contexts can accommodate comprehensive data protection legislation and ZTA-aligned architecture — directly countering the argument that Kuwait's regulatory trajectory is institutionally constrained.

8 Design Science Research Contributions

This section makes explicit the paper's contributions within the DSR framework, addressing the Discover Computing expectation for clearly stated computing research contributions.

8.1 Artefact Contribution: The CRGMM as a Cyber Risk Engineering Framework

The CRGMM constitutes the primary computing artefact of this paper. As a DSR artefact, it contributes: (1) a novel problem framing — the governance-technology disjunction in platform e-government — as an engineering problem requiring a measurable assessment instrument, not merely a policy recommendation; (2) a formally operationalised assessment instrument — six dimensions, five levels, fourteen GQM-derived indicators — with defined assessment methods enabling reproducible scoring by independent assessors; and (3) preliminary empirical grounding — expert panel validation (n = 15, alpha = 0.76) and pilot application to Kuwait's Sahel platform providing proof-of-concept scoring.

8.2 Theoretical Contribution: ZTA Extensions for Government Platform Contexts

This paper develops three novel ZTA extensions applicable to citizen-facing government platforms that are not addressed in enterprise-oriented ZTA literature (NIST SP 800-207; CISA, 2023). These constitute a theoretical contribution to computing security architecture research: (1) citizen-endpoint heterogeneity — ZTA access controls must incorporate variable device capability and digital literacy as continuous risk-scoring inputs; (2) sovereign inter-agency integration — jurisdictional complexity across independent government entities requires federated ZTA policy enforcement distinct from enterprise policy enforcement mechanisms; and (3) biometric irreversibility — ZTA authentication frameworks for government platforms must incorporate biometric template protection requirements (NIST SP 800-76) as a non-reversible credential category requiring categorically distinct architectural protection.

8.3 Methodological Contribution: Quantitative Risk Scoring for Governance-Level Assessment

The cyber risk severity matrix (Table 2) demonstrates that governance-level cyber risk assessment — traditionally treated as qualitative — can incorporate quantitative likelihood × impact scoring calibrated against observable governance indicators. This methodological contribution bridges the gap between qualitative framework analysis (common in digital governance research) and the quantitative risk scoring expected in computing and cybersecurity engineering publications. The matrix is reproducible: the scoring methodology is explicitly stated and can be updated as new threat intelligence or platform architecture disclosures become available.

8.4 Comparative Contribution: First Multi-Platform ZTA Benchmarking for GCC E-Government

The six-dimension comparative benchmarking of Sahel against UAE PASS, Estonia X-Road, Singapore SingPass/NDI, and Saudi Absher (Table 8) constitutes the first systematic ZTA-focused comparison of GCC and international digital government platforms in the peer-reviewed literature. This comparative contribution provides: a transferable benchmarking methodology applicable to future platform e-government comparisons; specific architectural patterns from leading platforms that are directly transferable to Kuwait's reform agenda; and empirical demonstration that the governance architecture gaps are not structurally inevitable in Gulf institutional contexts.

9 Policy Propositions and Cyber Risk Engineering Reform Roadmap

Drawing on the preceding analysis, we derive ten policy propositions. Table 9 presents these propositions in structured form, sequenced across three reform phases.

Table 9. Policy Propositions, Mechanisms, Theoretical Bases, and CRGMM Impacts

Ref	Reform	Mechanism	Theoretical Basis	CRGMM Impact	Phase

P1	Data Protection Legislation	Enact comprehensive PDPL: lawful bases, purpose limitation, data minimisation, data-subject rights, biometric-specific provisions	Regulative pillar (Scott, 1995); PbD Principles 2, 3, 7	D1, D5: 1–1.5 → 3+	Phase 1 (0–18 months)
P2	Independent Data Protection Authority	Establish DPA with powers to investigate, sanction, and issue binding guidance on government data processing	Coercive institutional pressure (DiMaggio & Powell, 1983); risk governance legitimacy (Renn, 2008)	D1, D2: 1.5–2 → 3+	Phase 1 (0–18 months)
P3	Platform Incident Response Mandate	CITRA to mandate and publicly disclose platform IRP — detection triggers, 72-hour citizen notification, designated incident commander	NIST CSF 2.0 Respond/Recover; Normal Accident Theory (Perrow, 1984)	D4: 1 → 3+	Phase 1 (0–18 months)
P4	Business Continuity & Resilience Architecture	Commission and disclose platform resilience architecture; test annually against DDoS, ransomware, and cloud-failure scenarios; publish RTO/RPO	Normal Accident Theory decoupling; NIST CSF Recover; ISO 22301	D4: 1 → 3	Phase 2 (18–36 months)
P5	Mandatory Privacy Impact Assessments	All new service integrations subject to PIA per ISO 29134 before approval; register published quarterly	PbD proactive principle (Cavoukian, 2009); GDPR Article 35 analogue	D5: 1.5 → 3	Phase 1 (0–18 months)
P6	Government-Wide TPRM Standard	Publish mandatory C-SCRM standard per NIST SP 800-161 Rev.1: min. security reqs, audit rights, breach notification, SBOM requirements, exit clauses	NIST SP 800-161 Rev. 1; ISO 27001 A.15; cloud shared-responsibility model	D2, D3: → Level 3	Phase 1 (0–18 months)
P7	Proactive Anti-Fraud Infrastructure	Extend Aman to active defence: automated phishing-domain OSINT, app-store takedown SLAs, published response-time metrics; modelled	NCSC Active Cyber Defence precedent; NIST CSF Detect/Respond; MITRE ATT&CK T1566	D3, D6: → Level 3	Phase 2 (18–36 months)

		on NCSC Active Cyber Defence			
P8	Biometric Data Protection Regime	Statutory and technical framework for Hawyti: lawful bases, encryption-at-rest standards, cross-agency access controls, objection rights, mandatory deletion timelines	Biometric irreversibility; PbD end-to-end security; ZTA identity tenet; NIST SP 800-76	D5: → Level 3+	Phase 2 (18–36 months)
P9	Mandatory ISO 27001 Certification	All integrated agencies: ISO 27001:2022 certification within 36 months; published compliance register updated quarterly; weakest-link audit provision	Normative institutional pillar; Normal Accident Theory (weakest-link)	D3: all agencies → Level 3	Phase 2 (18–36 months)
P10	Structured Citizen Cyber-Literacy Programme	Multilingual (Arabic, English + ≥ 2 further languages) digital-literacy programme; behavioural-nudge onboarding; annual uptake metrics published	Citizen enablement as legitimacy condition; ENISA awareness frameworks; Renn (2008) stakeholder deliberation	D6: 2 → 3+	Phase 3 (36–60 months)

Note: Phase 1 (amber) = 0–18 months: legislative and accountability foundation. Phase 2 (green) = 18–36 months: technical standardisation and resilience architecture. Phase 3 (blue) = 36–60 months: continuous governance and citizen enablement.

10 A Sequenced Reform Agenda: Governance Architecture Before Operational Expansion

The ten propositions cannot be implemented simultaneously. We propose a three-phase agenda organised around the foundational principle that governance architecture must precede — not follow — operational capability expansion.

10.1 Phase 1 (0–18 Months): Legislative and Accountability Foundation

Phase 1 establishes the non-negotiable legal and institutional foundations without which all subsequent technical and operational controls lack enforceability and legitimacy. Priority actions: enact a comprehensive personal data protection statute (P1); establish an independent Data Protection Authority (P2); mandate and publicly disclose a platform-level incident response plan with 72-hour citizen notification obligations (P3); publish a government-wide TPRM standard (P6); and mandate PIAs for all pending service integrations (P5).

10.2 Phase 2 (18–36 Months): Technical Control Standardisation and Resilience Architecture

Phase 2 builds the technical control architecture on the Phase 1 legislative foundation. Priority actions: commission and disclose the platform resilience architecture and BCP (P4); mandate ISO 27001:2022 certification across all integrated agencies (P9); publish the biometric data protection framework per NIST SP 800-76 (P8); and extend Aman to active cyber defence (P7). The ZTA architecture mandate for all inter-agency API integrations — requiring OAuth 2.0/OIDC federation, API gateway protection, and microsegmentation — should be formalised in this phase, operationalising the proposed architecture shown in Figure 2.

10.3 Phase 3 (36–60 Months): Continuous Governance and Citizen Enablement

Phase 3 institutionalises continuous governance and expands citizen enablement. Priority actions: operationalise the structured multilingual digital-literacy programme (P10); and establish the CRGMM as a regular public reporting instrument — publishing Kuwait's platform cyber governance maturity assessment annually with independent verification. Future work should empirically validate the CRGMM using cross-national digital government datasets and integrate quantitative cyber-risk analytics — including computational security metrics from platform telemetry — into platform governance assessment.

11 Discussion: Computing Contributions, Comparative Context, and Limitations

11.1 The Governance-Technology Disjunction as a Computing Research Problem

The structural disjunction between operational capability and governance architecture identified in Kuwait's case reflects a generalised pattern documented in computing research across cloud computing adoption (Almorsy et al., 2016), IoT governance (Sicari et al., 2015), and algorithmic public-sector decision-making (Misuraca & Viscusi, 2020). The CRGMM's contribution to computing research is to provide a measurable, indicator-based diagnostic instrument for this class of governance-technology problem, operationalising what existing maturity models treat as a binary (compliant/non-compliant) judgement into a reproducible maturity trajectory with fourteen quantitatively anchored scoring indicators.

11.2 Strengthening the Computing Literature Base

This paper's contribution is situated within an active computing and cybersecurity literature. Recent work on ZTA in government contexts includes Gilman and Barth (2017) on zero trust networks, He et al. (2022) on cybersecurity challenges in distributed systems, Chandramouli (2020) on ZTA for microservices-based applications, and Rose et al. (2020) on NIST SP 800-207. The maturity model literature includes Proença and Borbinha (2016) on information security maturity models, and Paulk et al. (1993) on the original CMMI framework. This paper contributes to both streams by developing a DSR artefact that bridges them for the platform e-government context — a bridge that neither stream has previously established.

11.3 GCC Comparative Context

The UAE PASS offers the closest GCC-contextual parallel, demonstrating that Gulf institutional contexts can accommodate comprehensive data protection legislation and ZTA-aligned architecture. However, the comparison should not be uncritical: UAE cyber governance, while structurally advanced, presents tensions around independent enforcement against government entities and civil society oversight. Legislative enactment is necessary but not sufficient — independent enforcement, civil society participation, and transparency reporting are the differentiating factors between formal and substantive cyber governance maturity.

11.4 Methodological Limitations

This paper's analysis is subject to four categories of limitation with specific implications for computing research credibility:

- Absence of penetration testing data: The threat taxonomy and control adequacy assessment are based on architectural analysis and public documentation. No penetration testing, red-team exercise data, or vulnerability scan results inform the technical risk assessments.
- Lack of internal architecture access: Sahel's internal API specifications, ZTA configuration, SIEM deployment, and data classification standards are not publicly available. Architecture assessments reflect published disclosures and are subject to revision if internal documentation were accessible.
- No empirical attack simulation: The CRGMM scoring for Technical Control Maturity is based on governance-observable indicators, not empirical attack simulation or independent security audit.
- Limited operational telemetry: The absence of publicly disclosed incident data, MTTD metrics, or security operations telemetry prevents empirical validation of the threat taxonomy's risk severity assessments. This limitation is compounded by the transparency deficit identified as a governance problem in Section 5.4.

These limitations are partly constitutive of the research problem: the transparency deficit that limits assessment precision is the same transparency deficit that the paper's reform propositions seek to address.

12 Conclusion

This paper has developed and preliminarily evaluated the CRGMM — a cyber risk engineering framework for multi-agency digital government platforms — using Kuwait's Sahel platform as a proof-of-concept application case. Five substantive findings emerge.

First, Sahel's platform consolidation creates the concentration paradox — constituting a systemically important government platform (SIGP) requiring governance obligations commensurate with its systemic importance. STRIDE and MITRE ATT&CK analysis identifies five primary attack surfaces; quantitative risk scoring identifies platform identity fraud and cross-agency data breach as critical-band risks (score = 20).

Second, evaluation against NIST CSF 2.0, ISO/IEC 27001/27701, and Privacy by Design reveals adequate technical controls at the authentication layer but critical gaps in ZTA implementation, incident response, business continuity, data governance, and citizen transparency. The absence of a personal data protection statute and independent supervisory authority constitutes a structural legislative deficit with direct computing-architecture implications.

Third, the CRGMM provides a DSR artefact — operationalised through six dimensions and fourteen measurable indicators, preliminarily validated through an expert panel achieving Krippendorff's alpha = 0.76 — that explicitly distinguishes technical control maturity from governance maturity. The formal comparison with CMMI, NIST CSF tiers, CISA ZTA MM, CMMC, and C2M2 (Table 4) demonstrates that no existing model addresses all nine design dimensions required for platform e-government assessment.

Fourth, international benchmarking against UAE PASS, Estonia X-Road, Singapore SingPass/NDI, and Saudi Absher confirms that governance architecture gaps are not structurally inevitable, and identifies specific transferable technical patterns. Two architecture diagrams (Figures 1 and 2) operationalise the CRGMM and proposed ZTA architecture as visual computing artefacts.

Fifth, the ten policy propositions and three-phase sequenced reform engineering roadmap make the central argument operational: governance architecture must precede operational capability expansion. Future work should conduct full Stage 2 and Stage 3 validation of the CRGMM using cross-national digital government datasets and integrate computational security metrics into platform governance assessment.

Declarations

Conflict of Interest: The author declares that there is no conflict of interest regarding the publication of this paper.

Ethical Approval: This study combined documentary analysis of publicly available sources with a structured expert panel evaluation conducted for artefact validation within a Design Science Research (DSR) methodology. The expert evaluation collected professional opinions on the relevance and adequacy of the proposed framework and did not involve sensitive personal data, vulnerable participants, or interventions. Participation was voluntary and responses were anonymised. In accordance with institutional and national guidelines for minimal-risk research involving expert professional judgement, formal ethics committee approval was not required.

Consent to Participate: All expert panel participants were informed about the purpose of the study, the voluntary nature of participation, and the anonymous treatment of responses. Informed consent to participate was obtained from all participants involved in the expert evaluation.

Consent to Publish: All participants provided informed consent for the anonymised and aggregated publication of the study findings. No personally identifiable information is reported in this manuscript.

Data Availability: The documentary and secondary data used in this study are publicly available and cited in the reference list. The expert panel data were collected anonymously and are available from the corresponding author upon reasonable request, subject to confidentiality considerations.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

Al-Enezi, J. (2019) Digital identity and non-citizen governance in Kuwait: administrative practice and civil rights implications. Arab Law Quarterly, 33(4), 322–349.

Al-Khouri, A.M. (2022) Governance reform in the GCC: digital government, institutional capacity, and the regulatory pacing problem. Public Administration and Development, 42(3), 201–218.

Almorsy, M., Grundy, J. and Müller, I. (2016) An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

Alshehab, A., Alfayly, A. and Alazemi, N. (2025) Citizens' electronic satisfaction factors with digital government services: an empirical study from Kuwait. International Journal of Electrical and Computer Engineering, 15(2), 1452–1465.

Arab Times (2024) CITRA launches new service 'Aman' to combat e-fraud through Sahel. Arab Times Online. https://www.arabtimesonline.com (Accessed: 20 February 2026).

Basili, V., Caldiera, G. and Rombach, H.D. (1994) The goal question metric approach. In: Encyclopedia of Software Engineering. New York: Wiley, 528–532.

Cavoukian, A. (2009) Privacy by Design: The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario.

Chandramouli, R. (2020) Building Secure Microservices-based Applications Using Service-Mesh Architecture. NIST SP 800-204A. Gaithersburg, MD: NIST.

CISA (Cybersecurity and Infrastructure Security Agency) (2023) Zero Trust Maturity Model Version 2.0. Washington, DC: U.S. Department of Homeland Security.

Collingridge, D. (1980) The Social Control of Technology. London: Frances Pinter.

DiMaggio, P.J. and Powell, W.W. (1983) The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160.

Dinev, T. and Hart, P. (2006) An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80.

Gilman, E. and Barth, D. (2017) Zero Trust Networks: Building Secure Systems in Untrusted Networks. Sebastopol, CA: O'Reilly Media.

Gong, Y., Yang, J. and Shi, X. (2023) Designing boundary resources in digital government platforms for cross-agency collaboration. Government Information Quarterly, 40(1), 101774.

Google Play (2024) Sahel — Apps on Google Play. https://play.google.com/store/apps/details?id=kw.gov.sahel (Accessed: 20 February 2026).

Gupta, P., Bhattacherjee, A. and Dugar, M. (2025) Trust, risk, privacy and security in e-government use: a meta-analysis and systematic review. Information Systems and e-Business Management, 23(1), 45–89.

He, Y., Aliyu, A., Evans, M. and Luo, C. (2022) Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. Journal of Medical Internet Research, 23(4), e21747.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004) Design science in information systems research. MIS Quarterly, 28(1), 75–105.

International Organization for Standardization (2019) ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Geneva: ISO.

International Organization for Standardization (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems. Geneva: ISO.

International Organization for Standardization (2023) ISO/IEC 29134:2023 Information technology — Security techniques — Guidelines for privacy impact assessment. Geneva: ISO.

International Risk Governance Council (2005) White Paper on Risk Governance: Towards an Integrative Approach. Geneva: IRGC.

Krippendorff, K. (2004) Content Analysis: An Introduction to Its Methodology. 2nd edn. Thousand Oaks, CA: Sage.

Kuwait Times (2024a) Kuwait 'Sahel' app transactions hit 110 million: Cabinet. Kuwait Times. https://kuwaittimes.com (Accessed: 20 February 2026).

Kuwait Times (2024b) Kuwait moves from fragmented govt services to integrated digital journeys. Kuwait Times. https://kuwaittimes.com (Accessed: 20 February 2026).

Microsoft (2006) The STRIDE Threat Model. Microsoft Security Development Lifecycle (SDL). Redmond, WA: Microsoft Corporation.

Misuraca, G. and Viscusi, G. (2020) Digital governance in the EU: from theory to practice in the public sector. Transforming Government: People, Process and Policy, 14(1), 7–22.

MITRE Corporation (2023) MITRE ATT&CK Enterprise Matrix v14. https://attack.mitre.org (Accessed: 20 February 2026).

National Institute of Standards and Technology (2020) NIST Special Publication 800-207: Zero Trust Architecture. Washington, DC: U.S. Department of Commerce.

National Institute of Standards and Technology (2021) NIST Special Publication 800-76-2: Biometric Specifications for Personal Identity Verification. Washington, DC: U.S. Department of Commerce.

National Institute of Standards and Technology (2022) NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Washington, DC: U.S. Department of Commerce.

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework 2.0. Washington, DC: U.S. Department of Commerce.

Paulk, M.C., Curtis, B., Chrissis, M.B. and Weber, C.V. (1993) Capability maturity model, version 1.1. IEEE Software, 10(4), 18–27.

Perrow, C. (1984) Normal Accidents: Living with High-Risk Technologies. New York: Basic Books.

Proença, D. and Borbinha, J. (2016) Information security management systems — a maturity model based on ISO/IEC 27001. In: International Conference on Business Information Systems. Cham: Springer, 102–114.

Renn, O. (2008) Risk Governance: Coping with Uncertainty in a Complex World. London: Earthscan.

Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: NIST.

Scott, W.R. (1995) Institutions and Organizations: Ideas, Interests, and Identities. Thousand Oaks, CA: Sage.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015) Security, privacy and trust in Internet of Things: the road ahead. Computer Networks, 76, 146–164.

Taddeo, M. and Floridi, L. (2018) The debate on the moral responsibilities of online service providers. Science and Engineering Ethics, 24(6), 1575–1603.

Times Kuwait (2024) Kuwait launches 'Smart Journeys' to bring government services closer to citizens. Times Kuwait. https://timeskuwait.com (Accessed: 20 February 2026).

Tiwana, A., Konsynski, B. and Bush, A.A. (2010) Platform evolution: coevolution of platform architecture, governance, and environmental dynamics. Information Systems Research, 21(4), 675–687.

UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (2021). Official Gazette of the United Arab Emirates.

Venable, J., Pries-Heje, J. and Baskerville, R. (2012) A comprehensive framework for evaluation in design science research. In: International Conference on Design Science Research in Information Systems. Berlin: Springer, 423–438.

Wieringa, R.J. (2014) Design Science Methodology for Information Systems and Software Engineering. Berlin: Springer.

Wippel, S. (2012) Regionalizing Oman: Political, Economic and Social Dynamics. Dordrecht: Springer.
World Bank (2025) The Gulf's Digital Transformation: Enabling Policies and Institutional Reforms. Washington, DC: World Bank Group.