© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722199

Cyber Risk Management and Compliance Readiness for Large-Scale Smart City Infrastructure

MUNIR AHMED MOHAMMED
0009-0000-7623-2535

Abstract- ***Large-scale smart city infrastructure is emerging as a strategic urban asset; however, it also expands the attack surface by interconnecting mobility platforms, utilities, public safety systems, data exchanges, cloud services, operational technology, and artificial intelligence-enabled decision services. Cyber risk management in this context cannot be approached as a periodic audit exercise, as disruptions may simultaneously impact safety, privacy, service continuity, public trust, and regulatory compliance. This review develops a compliance-readiness framework for smart city infrastructure by synthesising recent literature and control guidance published between 2020 and 2025. The study examines cyber risk across assets, data, identities, vendors, operational technology, cloud platforms, incident response, and governance evidence. It contends that readiness depends on the integration of risk registers with technical controls, control ownership, verification evidence, incident rehearsals, and board-level decision-making. The paper presents a structured architecture and an operating cycle intended to guide city authorities, project owners, technology integrators, and critical service operators throughout planning, procurement, commissioning, and operational phases. The review concludes that resilient smart city programmes require risk-based design, zero-trust access, privacy-aware data governance, secure-by-design procurement, continuous monitoring, tested recovery procedures, and measurable compliance evidence. These capabilities are particularly essential for Saudi smart city programmes aligned with digital transformation, national cybersecurity priorities, and Vision 2030.***

Keywords: Smart City Infrastructure, Cyber Risk Management, Compliance Readiness, Cyber Resilience, Data Governance, Operational Technology, Cloud Security, Saudi Arabia, Vision 2030

I. INTRODUCTION

Smart cities are no longer limited to isolated applications such as traffic sensors or mobile parking services. They increasingly operate as large cyber-physical ecosystems in which transport, buildings, surveillance, utilities, public spaces, logistics, healthcare interfaces and administrative services depend on shared data platforms and always-on connectivity. The technical value of this model is clear: city operators can use real-time data to improve asset utilisation, reduce congestion, detect hazards and coordinate service delivery. Yet the same interconnection also increases cyber exposure because a weak device, poorly governed data flow or vulnerable supplier interface can affect multiple services at once [1,2].

The risk profile of large-scale smart city infrastructure differs from that of ordinary enterprise information technology. Smart city systems combine constrained Internet of Things devices, cameras, control systems, cloud workloads, edge gateways, digital identity, analytics engines and operational command centres. Many components are deployed in public areas, connected through heterogeneous networks and maintained by several contractors. Risk therefore emerges not only from malware or unauthorised access, but also from fragmented accountability, unclear data ownership, untested recovery procedures, weak vendor assurance and incomplete visibility across information technology and operational technology boundaries [3-5].

Compliance readiness is equally complex. A smart city programme must demonstrate alignment with cybersecurity controls, privacy rules, data classification requirements, cloud obligations, critical system controls and sector-specific expectations. In Saudi Arabia, these obligations are shaped by national cybersecurity and data governance instruments, including controls for cloud services, data protection and critical systems [6-10]. Globally, risk-based frameworks such as the Cybersecurity Framework, zero-trust architecture and supply-chain risk management guidance emphasise governance,

identity, detection, response and recovery as continuous practices rather than one-time certification activities [11-14].

This review addresses the central question of how cyber risk management and compliance readiness can be organised for large-scale smart city infrastructure to ensure that technical security, regulatory evidence, and operational resilience are mutually reinforcing. The aim is to develop a practical conceptual framework that links smart city architecture with cyber risk domains, control objectives, readiness evidence, and assurance mechanisms. The objectives are to synthesise recent research on smart city cybersecurity, classify the principal risk and compliance readiness dimensions, propose a control-oriented architecture, and identify implementation priorities for Saudi smart city and giga-project environments.

II. METHODOLOGY

This paper employs a structured review design appropriate for a conceptual study in cybersecurity and governance. The review does not constitute a technical penetration test, legal opinion, or single-city case study. Instead, it synthesises recent literature and control guidance related to smart cities, cyber resilience, privacy, operational technology, cloud security, Internet of Things security, critical infrastructure assurance, and compliance readiness. Sources from 2020 to 2025 were prioritised to reflect current practices, prevailing threat conditions, and recent regulatory developments. Older foundational works were referenced only when necessary for terminology and were not used as primary citations.

The review proceeded in four stages. First, the topic was bounded around large-scale smart city infrastructure rather than consumer smart home devices or isolated municipal applications. Second, the literature was grouped into technical security, data governance, operational resilience, regulatory compliance, procurement assurance and critical infrastructure continuity. Third, each theme was examined for the controls, evidence and decision rights required to move from policy statements to operational readiness. Fourth, the synthesis was converted into a framework that can be used by project owners, chief information security officers, engineering managers, vendors, auditors and city-level decision makers.

The inclusion criteria prioritised sources addressing practical control implementation, risk assessment, architecture, monitoring, privacy, incident response, or assurance. General discussions of digital transformation were excluded unless they presented explicit cybersecurity or compliance implications. Studies focused solely on algorithm performance were also excluded unless they addressed security, privacy, resilience, or regulatory risk. This approach supports the central argument of the paper: smart city readiness is achieved when security controls are measurable, evidence is available, responsibilities are assigned, and recovery procedures are tested.

The synthesis is guided by three analytical questions: Which assets and data flows generate the highest city-level exposure? Which controls and governance mechanisms render these exposures manageable? What evidence demonstrates that controls operate effectively under normal, degraded, and incident conditions? These questions support a readiness perspective that extends beyond a checklist approach. A compliant smart city is not simply a programme with policies; it is a functioning ecosystem in which risks are identified, prioritised, monitored, reported, and mitigated through accountable engineering and operational practices [11,15].

Quality control was applied during synthesis by checking that each argument connected to the research question and that recommendations could be translated into implementation actions. This reduced descriptive drift and kept the review focused on readiness, evidence and risk ownership rather than general digital transformation benefits.

This perspective is particularly significant for large programmes delivered through multiple packages, as controls must remain coherent when separate contractors provide sensing, connectivity, platforms, operations, and maintenance workstreams across varying timelines. Consequently, evidence must be associated with the service rather than solely with the contract, and governance must ensure that design assumptions remain transparent as ownership transitions from construction teams to long-term

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722199

operators and city-level assurance functions during ongoing operations.

Table 1. Review protocol and analytical framework for cyber risk and compliance readiness.

Review stage	Evidence focus	Analytical question	Framework output
Problem framing	Smart city infrastructure, cyber-physical services, compliance exposure	Which services and data flows create city-level risk?	Scope boundaries and risk domains
Theme mapping	IoT, OT, cloud, data governance, identity, vendors and incident response	Which controls are required to manage risk?	Control categories and readiness dimensions
Compliance translation	National controls, privacy obligations, cloud controls and global standards	How are obligations converted into testable evidence?	Control evidence and assurance model
Operational synthesis	Monitoring, resilience, recovery, supplier assurance and reporting	How can readiness be sustained after launch?	Operating cycle and implementation priorities

III. SMART CITY INFRASTRUCTURE AS A CYBER-PHYSICAL RISK SYSTEM

Large-scale smart city infrastructure should be understood as a layered system. At the physical layer, sensors, meters, cameras, access devices, lighting assets, vehicles, substations, pumps and environmental systems collect signals and perform actions. At the connectivity layer, public networks, private 5G, fibre links, Wi-Fi, low-power networks and industrial protocols move data between city assets and operating platforms. At the platform layer, cloud environments, edge nodes, data lakes, digital twins, artificial intelligence services and dashboards convert raw data into operational decisions. At the governance layer, policies, roles, audit logs, contracts, privacy notices, control baselines and incident processes determine how the infrastructure is trusted.

This layered structure creates several risk concentrations. First, device scale makes inventory and patch management difficult. A city may contain thousands of endpoints distributed across roads, buildings and public spaces. Second, public exposure increases the likelihood of physical tampering, rogue maintenance access and unauthorised radio interaction. Third, data aggregation can transform seemingly harmless operational readings into sensitive behavioural profiles. Fourth, artificial intelligence models used for triage, surveillance, mobility or maintenance may introduce bias, opacity and dependence on data quality. Fifth, third-party operators may hold privileged access to systems that remain accountable to the city owner [1,3,16].

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722199

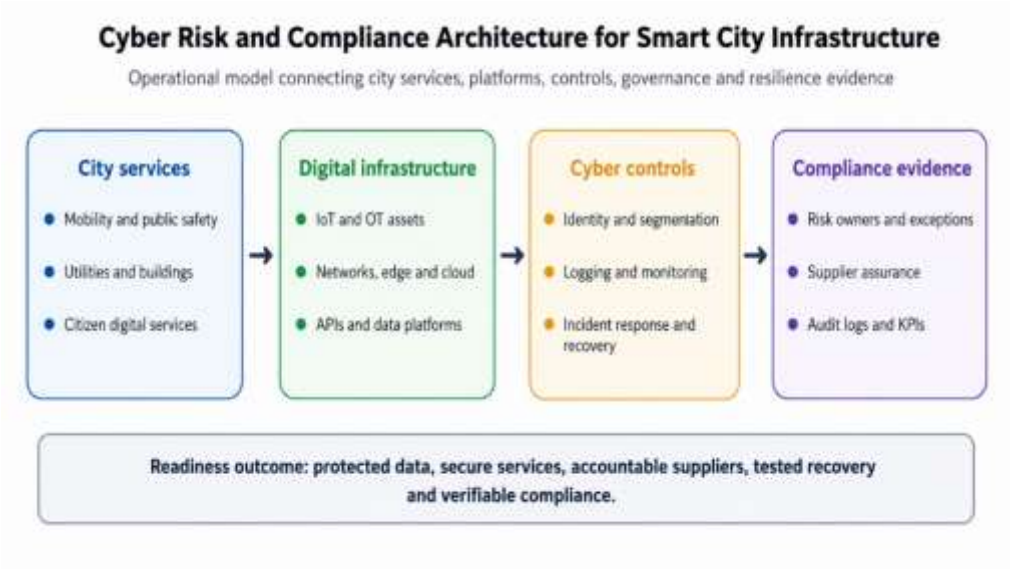

Figure 1. Cyber risk and compliance architecture for large-scale smart city infrastructure.

The compliance challenge is to translate broad requirements into concrete design and operating controls. Data minimisation, for example, must become retention rules, masking logic, role-based access, consent records and deletion procedures. Incident reporting obligations must become detection playbooks, severity thresholds, escalation contacts, evidence preservation and reporting clocks. Cloud security requirements must become data residency checks, tenant configuration baselines, encryption, key management, privileged access controls and supplier audit rights. Without this translation, compliance remains detached from engineering decisions and cannot support actual resilience [8,12,17].

The Saudi context strengthens the need for this integrated view. Large urban projects are expected to combine tourism, entertainment, mobility, energy, public safety and digital government services at high scale. These environments must support innovation while protecting critical information infrastructure, personal data, cloud workloads and operational continuity. The goal is therefore not to slow smart city adoption, but to make adoption governable. Cyber risk management should be embedded before procurement, during design approval, during commissioning and throughout operations, so that security is built into architecture rather than retrofitted after deployment [6-10].

IV. CYBER RISK LANDSCAPE

The first major risk domain is asset visibility. Many cyber failures begin with unknown systems, unmanaged devices, expired certificates, orphaned accounts or undocumented network paths. Smart city programmes multiply this problem because ownership is distributed among public authorities, master developers, contractors, cloud providers, facility operators and equipment vendors. Asset discovery must therefore cover hardware, software, firmware, data stores, interfaces, service accounts, digital certificates, network zones and physical locations. A risk register that does not include these dependencies will underestimate exposure and will fail during incident response [4,13,18].

Visibility must also distinguish business ownership from technical custody. A mobility platform may be owned by a transport authority, hosted by a cloud tenant, maintained by a vendor and used by emergency planners. Each party may see only part of the risk unless governance joins their evidence. For this reason, every critical service should have a service map showing assets, interfaces, owners, data classes, monitoring sources, supplier dependencies and recovery options. The map becomes the bridge between urban service management and cybersecurity assurance.

The second domain is identity and access. Smart city infrastructure depends on human users, machine identities, application programming interfaces, contractors, maintenance engineers, emergency operators and automated services. Traditional perimeter trust is unsuitable where assets are remote, mobile, cloud-hosted or vendor-managed. Zero-trust principles require explicit verification, least privilege, continuous access evaluation, segmentation and strong monitoring of privileged activity. These principles are particularly important for command dashboards, remote maintenance channels, camera platforms, building systems and traffic control interfaces, where misuse could affect safety or public confidence [12,19].

The third domain is data governance. Smart city data may include location traces, video, licence plates, biometric features, utility consumption, payment events, device telemetry, maintenance records and citizen service interactions. The risk increases when datasets are linked across domains because combined data can reveal behaviour even when individual fields appear operational. Readiness requires data classification, lineage, lawful purpose, minimisation, retention, anonymisation where appropriate, role-based sharing and independent review of high-risk processing. Privacy and cybersecurity must be treated as mutually reinforcing disciplines because weak security can become a privacy failure, while weak data governance can increase security impact [2,7,20].

The fourth domain is supplying chain and integration risk. Smart city projects commonly rely on global vendors, local systems integrators, managed service providers, equipment manufacturers and cloud platforms. Each relationship introduces configuration, access, support, update and evidence dependencies. Supplier contracts should require secure development, vulnerability disclosure, patch timelines, breach notification, subcontractor transparency, data location controls, audit rights and exit plans. Procurement should not ask only whether a solution is innovative; it should ask whether the solution can be operated securely for years under changing threat conditions [13,21].

The fifth domain is operational resilience. Large-scale smart city infrastructure cannot assume perfect prevention. It must continue essential services during degraded conditions and recover quickly after disruption. Resilience depends on logging, detection, backup, manual fallback, crisis communication, cyber exercises, recovery time objectives and tested restoration procedures. For operational technology and public safety systems, recovery planning must consider physical consequences, not only data restoration. The central readiness question is whether the city can make safe decisions when dashboards are unavailable, data integrity is uncertain or a supplier connection must be isolated [5,14,22].

V. COMPLIANCE READINESS FRAMEWORK

A compliance-readiness framework must connect governance intent to operational proof. The first layer is strategic governance. City authorities and project owners should define risk appetite, critical services, decision rights, regulatory obligations and assurance expectations. This layer sets the basis for prioritisation because not every asset requires the same depth of control. Systems affecting public safety, mobility continuity, utility operations, financial transactions, personal data or critical command functions require stronger evidence than low-risk public information services [11,14,23].

The second layer is architecture and control design. Controls should be mapped to infrastructure zones, data classes, service criticality and user roles. Typical controls include network segmentation, secure configuration, vulnerability management, identity governance, encryption, secure remote access, logging, endpoint protection, change management, backup and incident playbooks. In a smart city environment, these controls must be applied across the full technology stack, including field devices, edge gateways, cloud workloads, analytics platforms, digital twins and operator interfaces. Control design should be reviewed before vendor selection and again before operational handover [10,18,24].

The third layer is evidence management. Compliance readiness fails when evidence is manual, scattered or created only before an audit. Evidence should be generated as part of normal operations: asset inventories, access reviews, vulnerability dashboards, configuration baselines, change approvals, incident records, training completion, backup tests, supplier attestations and data protection assessments. Evidence should be attributable to owners, linked to risks and retained according to defined rules. This enables management to distinguish between controls that exist on paper and controls that operate in practice [15,17,25].

The fourth layer is continuous assurance. Smart city risk changes as new sensors are installed, buildings are commissioned, software is updated, APIs are added, contractors change and citizen services scale. Annual assessment alone is too slow. Continuous assurance combines automated monitoring, control testing, threat intelligence, red-team exercises, tabletop simulations, cyber drills and independent audits. The aim is to detect drift early and confirm that incident response, recovery and governance processes remain effective. Readiness should be measured through performance indicators, not only control counts [5,11,26].

The fifth layer is stakeholder accountability. Smart city cybersecurity involves city leadership, technology teams, urban planners, privacy officers, procurement teams, legal advisers, civil defence, emergency services, vendors, residents and regulators. Each group has different responsibilities and information needs. A practical framework should specify who owns each risk, who operates each control, who approves exceptions, who receives incident notifications and who validates evidence. This clarity reduces the coordination failures that often emerge when technical platforms are shared across organisational boundaries [1,23].

Readiness should also be assessed by maturity rather than by binary pass-or-fail language. At the initial level, a project may have policies and diagrams but limited evidence. At the developing level, controls exist for major platforms but are inconsistent across suppliers. At the managed level, controls are assigned to owners, tested and linked to risks. At the optimised level, evidence is automated, executive reporting is risk-based and lessons from incidents are fed into design standards. This maturity view allows leaders to prioritise resources where weak control operation creates the highest service or regulatory exposure [15,25,27].

A useful readiness model must also include exception management. Large projects rarely achieve perfect control alignment before launch, but exceptions should be explicit, time-bound, risk accepted and supported by compensating measures. Examples include temporary supplier access, legacy protocol use, delayed patch windows or interim data-sharing processes. Informal exceptions are dangerous because they hide risk from decision makers. Formal exceptions create a record of why a gap exists, who accepted it, how long it will remain and what monitoring is required while the gap is open [11,21].

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722199

Table 2. Cyber risk management and compliance readiness matrix for smart city infrastructure.

Readiness dimension	Key control focus	Required evidence	Readiness indicator
Asset and service visibility	Inventory, ownership, criticality, dependencies and exposed interfaces	Service maps, asset register, interface catalogue and ownership matrix	Critical assets mapped to owners and recovery options
Identity and access	Least privilege, strong authentication, privileged access, service accounts and supplier access	Access reviews, privileged session logs, joiner-mover-leaver records	High-risk access reviewed and exceptions time-bound
Data governance	Classification, minimisation, retention, encryption, lineage and sharing rules	Data flow diagrams, retention schedules, privacy reviews and approval records	Sensitive data flows documented and governed
Monitoring and response	SOC coverage, alert triage, incident playbooks, escalation and evidence preservation	Alert metrics, incident tickets, exercise reports and escalation records	Incidents triaged by city-level service impact
Supplier assurance	Security clauses, vulnerability handling, audit rights, subcontractor transparency and exit planning	Contract controls, attestations, patch reports and supplier risk reviews	Critical suppliers tested before operational handover
Recovery and resilience	Backup, fallback operations, restoration testing, crisis communication and lessons learned	Recovery test results, tabletop exercise records and corrective-action logs	Essential services recover within approved objectives

VI. IMPLEMENTATION PRIORITIES

Implementation should begin with a city-level risk baseline. The baseline should identify critical services, crown-jewel data, operational dependencies, external interfaces, supplier responsibilities and minimum control expectations. It should also identify services that cannot tolerate long outages, such as emergency coordination, access control, water, energy, mobility, communications and public safety monitoring. A baseline should be written in terms that executives, engineers and auditors can use, because cyber risk in smart cities is both a technical and governance matter.

The baseline should be updated at each project transition. During concept design, the focus should be criticality, data sensitivity and supplier model. During detailed design, the focus should shift to architecture diagrams, control allocation and integration risk. During commissioning, the focus should be test evidence, account hygiene, vulnerability closure and recovery rehearsal. During operations, the focus should be drift detection, incident learning and recurring assurance. This lifecycle approach prevents the common weakness where a secure design becomes insecure through later changes, emergency workarounds or undocumented integration [21,24].

A second priority is secure-by-design procurement. Many risks become expensive to correct after contracts are signed and platforms are deployed. Tender documents should request evidence of secure development, integration security, data protection, vulnerability handling, logging, identity federation, encryption, configuration management and resilience testing. Bidders should explain how their systems support regulatory reporting, audit logs, data retention, access reviews and secure decommissioning. Evaluation should include operational maintainability, not only functionality and cost [13,21,24].

A third priority is integrated monitoring. Smart city security operations should correlate network events, endpoint alerts, identity activity, cloud logs, operational technology anomalies, application errors, physical access events and supplier actions.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722199

Fragmented monitoring creates blind spots because attackers may move between environments. Monitoring should be supported by a documented escalation model that distinguishes technical severity from city-level impact. A camera outage, traffic signal compromise or water control anomaly may require different escalation than a conventional enterprise workstation alert [5,18,22].

A fourth priority is compliance engineering. Compliance requirements should be translated into control stories that engineers can implement and auditors can verify. For example, a data localisation requirement should become data flow diagrams, hosting decisions, backup locations, contractual restrictions and validation evidence. A privacy-by-design requirement should become minimisation, access control, retention schedules and high-risk processing reviews. A resilience requirement should become recovery objectives, failover designs, exercises and post-incident lessons. This translation prevents compliance from becoming disconnected paperwork.

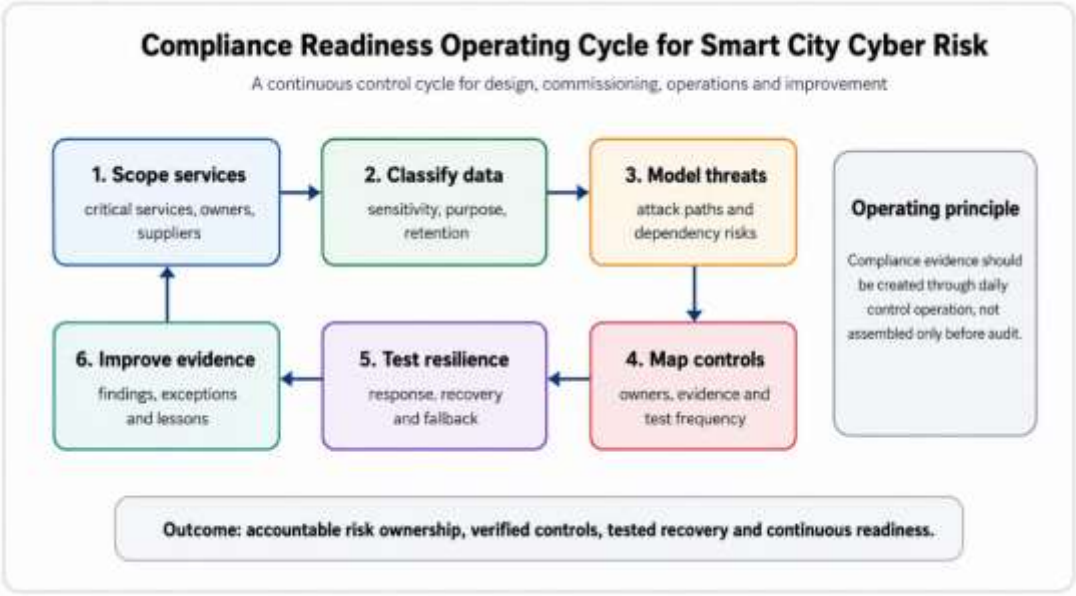

Figure 2. Compliance readiness operating cycle for smart city cyber risk management.

Compliance engineering should be supported by a common control library. The library should map each obligation to control objectives, technical safeguards, process safeguards, required evidence, test frequency and accountable roles. It should also identify which controls are inherited from cloud providers, which are operated by the city, which are operated by vendors and which require joint evidence. This distinction matters because shared responsibility can otherwise become shared ambiguity. A well-maintained library reduces duplicate assessments, improves procurement consistency and helps new projects reuse approved patterns without weakening assurance.

A fifth priority is scenario testing. Large-scale smart city programmes should test plausible disruptions before they occur. Scenarios may include ransomware against a city platform, compromise of a vendor remote access channel, loss of a cloud region, manipulation of sensor data, public disclosure of personal data, denial of service against citizen services, false alarms in public safety systems or loss of communications to operational assets. Scenario testing reveals whether roles, evidence, communications and fallback procedures are realistic [14,26,27].

A sixth priority is talent and governance maturity. Smart city cybersecurity requires expertise in networks, cloud, operational technology, privacy, incident response, architecture, contracts, urban operations and crisis management. No single team can

own all of this alone. Governance maturity depends on cross-functional forums, shared risk language, executive sponsorship, local capability development and routine reporting. Training should include not only technical controls, but also the responsibilities of contractors, project managers, control room staff and service owners.

A final implementation priority is post-incident learning. Smart city programmes should not wait for major incidents before improving controls. Near misses, failed access reviews, unsuccessful backup restorations, delayed vendor responses and recurring vulnerabilities all provide evidence about readiness. These signals should be reviewed through a formal lessons process and converted into changes to architecture standards, supplier clauses, monitoring rules and staff training. In this way, compliance becomes adaptive and learns from operational reality.

VII. DISCUSSION

The review shows that cyber risk management for smart cities should be framed as an operating discipline. A narrow compliance checklist may create temporary audit comfort, but it cannot keep pace with new services, new suppliers and new attack paths. Readiness becomes credible when city authorities can show what assets exist, how data move, who has access, how controls are tested, how incidents are escalated and how services recover. The strongest programmes treat compliance evidence as a by-product of disciplined operations.

There is also a trade-off between innovation speed and assurance depth. Smart city projects often face pressure to demonstrate visible digital progress. However, rapid deployment without security architecture can create hidden liabilities that later restrict integration, delay approvals or undermine trust. The framework proposed here does not argue for slowing innovation. Instead, it argues for sequencing innovation through risk gates: concept approval, design assurance, supplier validation, commissioning, operational monitoring and continuous improvement. Each gate should add clarity rather than bureaucracy.

Another finding is that compliance readiness is inseparable from public trust. Smart city residents may not see encryption, access controls or incident exercises, but they experience the consequences of weak governance through outages, intrusive data use or poor response to incidents. Public trust is strengthened when data purposes are clear, high-risk systems are governed, security responsibilities are transparent and critical services remain dependable. Therefore, cyber risk management should be linked to service quality, safety and legitimacy, not presented only as a technical cost centre [2,20,28].

The framework also highlights the importance of data integrity. In smart city operations, inaccurate or manipulated data can be as damaging as unavailable data. False traffic data may change mobility decisions, altered environmental readings may hide hazards, manipulated access logs may weaken investigations and poisoned training data may influence automated decisions. Integrity controls should therefore include trusted time, signed telemetry, validation rules, anomaly detection, separation of duties and reconciliation between independent data sources. These controls are particularly important where digital twins and artificial intelligence models guide physical operations [3,16,29].

Interoperability is another strategic concern. Large smart city programmes often connect systems built by different vendors at different times. Open interfaces are necessary for integration, but they can also create uncontrolled pathways if application programming interfaces are not inventoried, authenticated, rate-limited, logged and reviewed. A compliance-ready environment should maintain an interface catalogue that records purpose, owner, data class, authentication method, dependency, testing status and decommissioning date. This catalogue becomes essential during incidents because responders need to know which connections can be isolated without causing wider service harm [18,24].

For Saudi smart city and giga-project environments, the practical contribution is a readiness model that aligns national ambition with operational accountability. The most effective projects will build cybersecurity into master planning, engineering

design, data governance, procurement, operations and performance reporting. They will also make room for local cyber capability, supplier supervision and continuous lessons from incidents. This approach can support resilient digital infrastructure while enabling the innovation expected from new urban destinations and future economic zones [6,9,10].

VIII. FUTURE RESEARCH AGENDA

Future research should move beyond general security recommendations and examine operational evidence from real smart city deployments. More studies are needed on cyber risk metrics for integrated urban platforms, data lineage in multi-operator environments, security of digital twins, protection of artificial intelligence decision services, supplier concentration risk and recovery from city-scale cyber incidents. Research should also investigate how to quantify the relationship between cyber controls and service continuity, because city leaders need evidence that security investment reduces operational and social risk.

Research should also clarify how cyber risk is communicated to non-technical leaders. Dashboards often report vulnerability counts, patch percentages or alert volumes, yet these measures do not always explain whether essential city services can survive an incident. More useful reporting would connect security posture with impact pathways: which service is exposed, which population could be affected, which vendor dependency is involved, which recovery option exists and what decision is required. Such reporting can improve board oversight and make cybersecurity investment more defensible [5,11,30].

There is a particular need for Saudi-context studies. Future work should assess how national cybersecurity controls, data protection obligations and cloud security expectations can be translated into reference architectures for transport districts, entertainment destinations, public safety platforms, district utilities and integrated facility operations. Such research should use anonymised operational data where possible, including incident trends, control-test results, audit findings, recovery exercises and vendor performance. This would improve the evidence base for risk-based investment and reduce reliance on generic international assumptions [6-10].

Future work should also consider assurance automation. As smart city infrastructures scale, manual compliance tracking becomes insufficient. Control evidence can be collected from configuration repositories, identity platforms, vulnerability scanners, ticketing tools, cloud policy engines, backup systems and security information platforms. However, automation must be governed carefully. Evidence pipelines should be transparent, tamper-resistant and understandable to auditors. Automated compliance scoring should support judgement, not replace expert review or accountability.

IX. CONCLUSION

Large-scale smart city infrastructure creates important opportunities for service quality, operational efficiency and urban innovation, but it also concentrates cyber, privacy and compliance risks. The review demonstrates that these risks cannot be managed through isolated technical controls or periodic audit preparation. They require an integrated readiness model that connects architecture, data governance, identity, supplier assurance, monitoring, incident response, recovery and evidence management. The proposed framework positions compliance as an operational capability rather than an administrative afterthought.

The analysis further shows that the most important readiness gap is not always the absence of technology. Many cities can buy sensors, platforms, detection tools and cloud services, but they struggle to maintain consistent ownership, evidence, service mapping and supplier accountability across the whole ecosystem. A mature programme therefore treats cyber risk as a shared urban management function. It links engineering decisions with privacy duties, procurement obligations, operations monitoring and crisis governance so that cyber control becomes part of city performance.

For project owners and city authorities, the central recommendation is to identify the critical services and data flows first, then design controls, assign owners,

test scenarios and maintain evidence continuously. For technology providers, the recommendation is to build solutions that support auditability, secure configuration, vulnerability response and data governance from the beginning. For Saudi smart city programmes, the framework can help align innovation with national cybersecurity priorities, data protection requirements and the long-term trust needed for smart urban transformation. Cyber risk management should therefore be treated as a core design principle of future cities.

The paper also emphasises that readiness must remain measurable after launch. Smart city operators should continue validating access, testing recovery, reviewing suppliers, improving data protection and reporting risk in service language. This continuous discipline is what turns compliance from a document collection into a practical capability for safe, trusted and resilient urban digital infrastructure.

REFERENCES

[1] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 24(2), 393-414. https://doi.org/10.1007/s10796-020-10044-1

[2] Rizi, M. H. P., & Seno, S. A. H. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, 20, 100584. https://doi.org/10.1016/j.iot.2022.100584

[3] Kour, H., Karim, S., & colleagues. (2023). Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey. Sensors, 23(7), 3681. https://doi.org/10.3390/s23073681

[4] Anwar, R., & Ali, S. (2022). Smart cities security threat landscape: A review. Computing and Informatics, 41(2), 405-423. https://doi.org/10.31577/cai_2022_2_405

[5] European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. ENISA, Athens.

[6] National Cybersecurity Authority. (2020). National cybersecurity strategy. Kingdom of Saudi Arabia.

[7] Saudi Data and Artificial Intelligence Authority. (2024). Personal Data Protection Law implementing regulations. SDAIA, Riyadh.

[8] National Cybersecurity Authority. (2022). Data Cybersecurity Controls (DCC-1:2022). Kingdom of Saudi Arabia.

[9] National Cybersecurity Authority. (2024). Cloud Cybersecurity Controls (CCC-2:2024). Kingdom of Saudi Arabia.

[10] National Cybersecurity Authority. (2022). Operational Technology Cybersecurity Controls (OTCC-1:2022). Kingdom of Saudi Arabia.

[11] National Institute of Standards and Technology. (2024). The Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper, CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[12] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207

[13] Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST Special Publication 800-161 Revision 1. https://doi.org/10.6028/NIST.SP.800-161r1

[14] Cybersecurity and Infrastructure Security Agency. (2023). Cross-Sector Cybersecurity Performance Goals. CISA, Washington, DC.

[15] International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. ISO, Geneva.

[16] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST, Gaithersburg, MD. https://doi.org/10.6028/NIST.AI.100-1

[17] International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls. ISO, Geneva.

[18] Fagan, M., Marron, J., Brady, K., Jr., Cuthill, B., Megas, K., & Herold, R. (2021). IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. NIST Special Publication 800-213. https://doi.org/10.6028/NIST.SP.800-213

[19] Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model, Version 2.0. CISA, Washington, DC.

[20] Saudi Data and Artificial Intelligence Authority. (2020). National Data Governance Policies. SDAIA, Riyadh.

[21] National Institute of Standards and Technology. (2022). Secure Software Development Framework (SSDF), Version 1.1. NIST Special Publication 800-218. https://doi.org/10.6028/NIST.SP.800-218

[22] Cybersecurity and Infrastructure Security Agency. (2021). Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. CISA, Washington, DC.

[23] United Nations Human Settlements Programme. (2022). People-centered smart cities: A thematic guide. UN-Habitat, Nairobi.

[24] European Parliament and Council. (2024). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements. Official Journal of the European Union.

[25] The Institute of Internal Auditors. (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense. IIA, Lake Mary, FL.

[26] European Union Agency for Cybersecurity. (2023). Cybersecurity exercises: Good practice guide. ENISA, Athens.

[27] European Parliament and Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union.

[28] European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union.

[29] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors, 23(8), 4117. https://doi.org/10.3390/s23084117

[30] World Economic Forum. (2021). Governing smart cities: Policy benchmarks for ethical and responsible smart city development. WEF, Geneva.