



## Cloud Governance and Vendor Risk Management: A Case Study of Sri Lanka's NMRA Data Loss

Sahan Samarathunga\*, Anjula Handapangoda, Shehan N. Suraweera,  
Theekshani Hettiarachci, Madhushka Kumanayakage  
University of Kelaniya, Sri Lanka

Received: June 9, 2026

Revised : August 17, 2026

Accepted : October 13, 2026

Online : October 14, 2026

### Abstract

Digital transformation improves efficiencies but poses risks related to data sovereignty, vendor risk management (VRM), and information technology (IT) governance. The paper examines the data loss case at the National Medicines Regulatory Authority (NMRA) in Sri Lanka. In this incident, about two terabytes of pharmaceutical data were lost. The data included proprietary information and manufacturing approval of drugs obtained from the e-NMRA system in the Lanka Government Cloud. Prior studies have examined GRC frameworks adoption in mature settings and lacks explanation on how cloud governance and vendor oversight fail in low-capacity public sectors, addressing the gap this study examines. Using a qualitative single-case study design based on triangulation of documentary evidence (audit reports, parliamentary records, media investigations, and scholarly literature), the incident is evaluated against Governance, Risk, and Compliance (GRC) models, including ISO/IEC 27001 and COBIT 2019, and Heeks' design-reality gap (DRG) model. The analysis indicates that the loss is best explained by an undelivered disaster recovery solution, unmonitored vendor privileged access, an unclear shared-responsibility arrangement, and the absence of backups and audit trails, rather than by an attack. These findings demonstrate that GRC models assume institutional maturity and technical expertise, which may not hold in emerging digital economies. On this basis, the paper proposes the Sovereign Cloud Governance and Vendor Risk Management (SCG-VRM) model, derived from one case and requiring empirical validation. The model contributes by contextualising GRC and vendor risk management for developing public sectors, considering low institutional enforcement capability, vendor capture tendencies, and other emerging-economy peculiarities.

**Keywords** *Cloud Governance, Vendor Risk Management (VRM), Public Health Infrastructure, Digital Sovereignty, NMRA, COBIT 2019, ISO/IEC 27001, Design-Reality Gap.*

### INTRODUCTION

Cloud computing's incorporation into public sector activities has changed the norms of state administration worldwide. Providing efficient and scalable infrastructure, cost-effectiveness, and better delivery of services online, cloud computing systems have become the foundation for e-government strategies. Within the context of public health, cloud-based solutions allow managing electronic health records, national databases on regulations, and telemedicine services, increasing the speed of government reactions to public health crises such as the COVID-19 pandemic (World Bank, 2022). According to the World Bank, switching to cloud technology makes it possible for governments in developing nations to bypass traditional obstacles associated with the limited capacity of IT infrastructure, providing them with more advanced analytics and cybersecurity measures without having to allocate prohibitive capital resources (World Bank, 2022).

Outsourcing important data from developing countries into cloud environments developed, hosted, or controlled by external vendors entails several serious operational, security-related, and governance risks. Although cloud computing removes concerns about server management, it poses additional challenges for data governance. Lack of adequate and localized information technology

### Copyright Holder:

© Samarathunga, Handapangoda, Suraweera, Hettiarachci & Kumanayakage. (2026)  
Corresponding author's email: [samarat-cs20034@stu.kln.ac.lk](mailto:samarat-cs20034@stu.kln.ac.lk)

### This Article is Licensed Under:



governance structures makes the government highly vulnerable to issues such as vendor lock-in, violations of data sovereignty principles, compromised cloud supply chains, and potentially severe data loss (Rambau et al., 2026; Nfuka & Rusu, 2011). However transferring all the responsibility for technical operations to the vendor will not absolve the government of its legal and regulatory obligations related to vendor oversight, yet many public sector agencies lack such maturity (Rambau et al., 2026).

An example of such a potentially risky phenomenon is the case of data loss at the Sri Lankan NMRA. Statutorily mandated with the evaluation, regulation, and authorization of all drugs, medical devices, and borderline products to guarantee their safety and protect citizens from potential dangers, the NMRA is one of the core components of Sri Lanka's healthcare security (Auditor General's Department, 2021). Seeking to modernize its processes, the NMRA outsourced its digitalization needs to Epic Lanka Technologies, a private software company. Hosting the e-NMRA system on the state-controlled Lanka Government Cloud (LGC), the NMRA experienced a disastrous data deletion incident in July 2021, which led to the loss of about 2,000 gigabytes of highly confidential intellectual property and drug formulation and manufacturing authorizations submitted by international pharmaceutical companies (Auditor General's Department, 2021; Counterpoint, 2021). The data loss resulted in disruption of the country's drug registration pipeline and interrupted supply of essential medications, prompting several parliamentary and criminal investigations of the scandal (Parliament of Sri Lanka, 2021, 2024; Counterpoint, 2021).

This study addresses three research questions:

1. RQ1: What governance, vendor-risk, and operational-resilience weaknesses are documented in the 2021 NMRA data-loss incident?
2. RQ2: How can the documented weaknesses be interpreted using ISO/IEC 27001, COBIT 2019, and the Design-Reality Gap (ITPOSMO) framework?
3. RQ3: What context-sensitive governance mechanisms can be conceptually derived from the NMRA case to strengthen vendor accountability, operational sovereignty, and data resilience in public-sector sovereign cloud environments in developing economies?

Global models, including ISO/IEC 27001 and COBIT 2019, outline detailed approaches to securing supply chains in clouds, managing risks associated with third parties, and providing continuous business resilience (ISACA, 2019; Malatji, 2023). But, their application in public sectors in developing nations typically lacks rigour and suffers from inadequate financial resources as well as poor fit with socio-political, infrastructural, and legal realities in these nations (Rambau et al., 2026; Nfuka & Rusu, 2011). The concept of Design-Reality Gap (DRG) by Heeks sheds light on the reasons for these assumptions failing in developing nations (Heeks, 2003).

Hence, there is a need to conduct the research. Firstly, it will evaluate the technical and administrative failure points of the NMRA case against the established frameworks of GRC architecture and DRG model to see if strict compliance with these approaches could prevent the disaster. Secondly, understanding that imported models may be unsuitable for the particular institutional environment, a risk assessment and policy solution framework will be suggested. The proposed Sovereign Cloud Governance and Vendor Risk Model (SCG-VRM) seeks to ensure the sovereignty of data storage and processing while strengthening vendor responsibility and protecting critical data of state organizations outsourcing cloud infrastructure.

The objectives of the study are to:

1. O1: Examine the documented governance, vendor-risk, access-control, backup, and disaster-recovery weaknesses associated with the NMRA data-loss incident.
2. O2: Analyze these documented weaknesses against ISO/IEC 27001, COBIT 2019, and the Design-Reality Gap (ITPOSMO) framework to identify gaps between formal governance requirements and institutional operating realities.

3. O3: Develop a conceptually derived Sovereign Cloud Governance and Vendor Risk Management (SCG-VRM) model that responds to the governance weaknesses identified in the case and accounts for institutional capacity constraints in developing public-sector environments.

## LITERATURE REVIEW

Literature related to cloud computing and its applications in the public sector is extensive but rather scattered, including disciplines as varied as cybersecurity and public administration. The purpose of this section is to merge both spheres to lay out the theoretical groundwork needed to analyze the given NMRA incident.

### Cloud Computing and GRC in the Public Sector

The motivation behind governmental cloud computing initiatives lies in a growing need to renew legacy infrastructure ([World Bank, 2022](#)). There are various degrees of flexibility offered by cloud computing delivery services ranging from Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). With decreasing physical ownership and control over the infrastructure, the importance of GRC becomes evident ([Debreceeny & Gray, 2009](#) ; [ISACA, 2019](#)).

GRC frameworks play an important role in reconciling the rapid availability of EMRs in the public health sector with high demands for data security, integrity, and system availability. Frameworks such as the HITRUST CSF, NIST cybersecurity framework, and ISO 27799 have become the standard practice in securing healthcare data in the cloud ([Cloud Security Alliance \[CSA\], 2024](#)). Frameworks such as mentioned above help translate complex regulatory standards (HIPAA, GDPR) into IT controls. However, the efficiency of such frameworks depends greatly on the level of institutional maturity, and in developing nations, IT governance in the public sector struggles with fragmented institutional leadership, a lack of technical staffing, and misalignment with broader policy goals ([Alharbi et al., 2022](#); [Nfuka & Rusu, 2011](#)). Without GRC frameworks, there is a tendency towards misconfiguration and uncontrolled access ([Rambau et al., 2026](#); [Bena et al., 2024](#)). The existing solutions identify an important limitation: established GRC frameworks specify what organisations should control, but provide less explanation of how those controls can remain effective when public-sector institutions have limited technical expertise, weak internal monitoring capacity, and constrained enforcement capability. The novelty of the present study lies in examining GRC not only as a set of formal security requirements but also as a governance capability whose effectiveness depends on the institution's ability to implement, verify, and enforce those requirements. This distinction provides the basis for subsequently connecting GRC maturity with vendor dependency and the Design-Reality Gap in the NMRA case.

### Vendor Risk Management (VRM) in Cloud Architectures

Vendor risks arise as a result of outsourcing key functions to vendors. Thus, strong VRM processes are needed to address them. VRM is an ongoing governance practice. Essentially, it is about tying all third-party dependencies on organizational risks ([Faruq, 2024](#); [Boyens et al., 2022](#)). Cloud vendors present new challenges because of the need to grant them direct access to the database and privileged access levels, thereby opening a window for a possible chain reaction in cases of human error ([Gupta et al., 2024](#); [AlGhamdi et al., 2020](#)).

The COBIT 2019 framework recognizes these risks as a separate management objective (APO010, Managed Suppliers) where the organization is expected to define a set of supplier relationships, enforce SLAs, and monitor supplier performance and risk management posture ([ISACA, 2019](#); [ISACA, 2016](#)). On the other hand, the ISO/IEC 27001 standard contains specific controls (Annex A.15) aimed at ensuring secure relationships with suppliers, including regular

audits and strict integration of security considerations into vendor agreements ([Malatji, 2023](#)).

Despite the presence of these guidelines in relevant standards, practical experience shows that VRM in the public sector is often severely underdeveloped ([Faruq, 2024](#); [AlGhamdi et al., 2020](#)). Organizations fail to continuously monitor their vendors post-tender process and rely on one-time assessment of the vendor's security stance at the time of the purchase ([Faruq, 2024](#); [Al-Ansari & Alsubait, 2022](#)). Shared responsibility in clouds (where responsibilities between the cloud provider, the software vendor, and the client aren't clearly defined) makes the data recovery even more complicated ([ISACA, 2016](#)). The proposed SCG-VRM model considers vendor compliance as an operational condition that must be continuously evidenced through monitoring of access privileges, backup status, security controls, and SLA performance rather than assumed from the existence of contractual provisions.

### **Digital Sovereignty and Data Localization**

With information becoming increasingly recognized as a strategic asset of national significance, the notion of digital sovereignty has gained traction and become a key concern in national security policies, especially when dealing with oligopoly in hyperscale cloud services offered by several multinational companies ([Mitchell & Samlidis, 2021](#); [Floridi, 2020](#)). The definition of digital sovereignty centers around the country's self-determined control over the digital infrastructure, data storage, and technologies in use free from any foreign influence and extraterritorial jurisdiction (e.g., US CLOUD act) ([Irion, 2012](#); [Floridi, 2020](#)).

Countries pursue digital sovereignty by mandating localization of all government data and citizen-sensitive information by keeping them on localized infrastructure or "Sovereign Clouds" (national-level cloud infrastructure) ([Mitchell & Samlidis, 2021](#); [Leka, 2024](#)). France uses SecNumCloud certification for ensuring cloud infrastructure and data sovereignty. PDPL law in Saudi Arabia and localized purchasing procedures in Australia are examples as well ([Mitchell & Samlidis, 2021](#)). Finally, implementation of Lanka Government Cloud in Sri Lanka is an example of pursuing the idea of sovereign cloud to prevent citizen data and sensitive information from leaving the borders of the country ([ICTA, 2023](#)).

Despite being geographically localized, data alone do not constitute true operational sovereignty. If an entity requires data localization but still cannot govern the cloud infrastructure's security (thereby granting full administrative and architectural access to the cloud vendor), it loses control over its data ([Irion, 2012](#); [Floridi, 2020](#)). Operational sovereignty then means having full cryptographic control over data, preventing any unilateral actions of a vendor ([Floridi, 2020](#); [ICTA, 2023](#)). The existing literature on digital sovereignty suggests that national control over data cannot be reduced entirely to the geographical location of data storage. However, for public-sector cloud environments, an important governance implication remains that sovereignty must also be evaluated in relation to operational control over privileged access, backup infrastructure, recovery mechanisms, and external service providers. The novelty of this study is therefore to operationalise digital sovereignty at the cloud-governance level by asking not only where government data is stored, but also who possesses the technical authority to access, modify, delete, and recover that data.

### **E-Government Failure and the Design-Reality Gap**

To fully understand the problem of IT failure in developing nations we have to considering the sociopolitical context behind it. The seminal work by Heeks introduced the Design-Reality Gap model that was used extensively for analyzing problems in e-governments ([Heeks, 2003](#)). According to this model, e-government project fails (with an estimate of 35% overall and 50% partial failures in developing countries) when there is a substantial disjunction between

assumptions embedded in the system design and the realities of the public organization implementing it ([Heeks, 2003](#)).

These assumptions can be categorized into the following dimensions described using the ITPOSMO acronym: Information, Technology, Processes, Objectives and values, Staffing and skills, Management systems and structures, and Other resources (time and money) ([Heeks, 2003](#); [Heeks, 2006](#)). Empirical application of this model in research shows that soft issues (such as governance weaknesses, lack of skills, resistance to transparency, and interference of politics) prevail as the root causes of e-government failures regardless of the technical aspects ([Lessa et al., 2016](#); [Tamilarasi et al., 2024](#); [Nfuka & Rusu, 2011](#)). Analysis of technical problems, such as data deletion, should accordingly consider the DRG model. The study breakdowns institutional weakness into specific gaps in staffing and skills, management continuity, processes, resources, technology, objectives and values, and information governance, and examines how these gaps interact with vendor dependency and GRC weaknesses.

## RESEARCH METHOD

This research uses a qualitative single-case study methodology to study the NMRA data loss event. Single case studies are especially appropriate to deal with contemporary and multidimensional events where lines between the event itself and its context (both technical and social) are blurry. The study relies exclusively on secondary documentary evidence because interviews, direct system access, and system logs were not available. The purpose is therefore to reconstruct the documented sequence of events and examine the governance and vendor-risk weaknesses visible in that record.

### Statutory Audit Reports

The study uses statutory audit reports of the Auditor General's Department concerning NMRA performance during 2021–2024 ([Auditor General's Department, 2021](#); [Auditor General's Department, 2023](#)). These documents will serve as a basis for the assessment of management inefficiency and GRC weaknesses. These documents provide the main documentary basis for describing institutional actions, control weaknesses, backup and disaster-recovery findings, and other operational conditions recorded by the audit process.

### Parliamentary Oversight Documents

Parliamentary oversight records and statements released by the Committee on Public Enterprises (COPE) are used to examine institutional responses, reported responsibility for vendor and recovery arrangements, and issues raised during public oversight. ([Parliament of Sri Lanka, 2021](#); [Parliament of Sri Lanka, 2024](#)). Statements in these records are treated as recorded positions or allegations where the documentary record does not independently establish the underlying claim.

### Media and Cybersecurity Investigation Reports

Technical aspects of data deletion will be reconstructed through investigation reports in the media and expert cybersecurity publications ([Counterpoint, 2021](#)). These sources are not treated as equivalent to statutory records; where accounts differ, the study gives greater evidentiary weight to statutory audit and parliamentary records and attributes claims that rely on a single source.

## Research and Framework Literature

Findings obtained from secondary analysis will be assessed against existing academic literature on cloud computing, GRC and VRM standards and practices, and the DRG model ([ISACA, 2019](#); [Malatji, 2023](#) ; [Heeks, 2003](#)).

Document selection was purposive rather than exhaustive. Documents were included when they directly addressed the NMRA data-loss incident, the governance or contractual responsibilities of NMRA, ICTA, or Epic Lanka, the backup and disaster-recovery arrangements, or the institutional response to the incident. Sources were excluded where they merely repeated the incident without providing additional evidentiary or analytical value.

Analysis will begin with constructing a chronological narrative of the event in question and then identify weak points in the process that led to data deletion. These weak points will be mapped to different dimensions of the chosen frameworks. Second-order and third-order conclusions will allow us to formulate a SCG-VRM framework. The documentary record does not always provide identical accounts of responsibility. Rather than resolving such disagreements through assumption, the study reports the different positions and gives greater weight to statutory audit and parliamentary records when describing institutional actions. Claims that cannot be established beyond a single source are attributed to that source. The analysis also distinguishes documented evidence from interpretation: the documents can establish what occurred, what institutions recorded or stated, and what arrangements were reported, but they do not by themselves establish the motives or intentions of individual actors. The proposed SCG-VRM model is consequently presented as a conceptual governance response derived from the identified weaknesses, not as a validated or empirically tested solution.

## FINDINGS AND DISCUSSION

### System Architecture and Project Inception

The NMRA provides Sri Lanka with its healthcare security, being the only statutory body responsible for regulating and authorizing all pharmaceutical products and medical devices entering the Sri Lankan market ([Auditor General's Department, 2021](#)). Its old system was paper-based. Having identified inefficiencies and lack of visibility associated with the use of manual, paper-based process flow, the NMRA launched a digital transition process. In May 2018, as per the terms of a five-year project tender award, the NMRA assigned a contract to Epic Technology Group (often referred to as Epic Lanka), a prominent local software provider with a specialization in public sector and financial industry IT products, to provide the development and maintenance of the e-NMRA workflow and document management solution ([Auditor General's Department, 2021](#)).

Adhering to Sri Lankan national digital sovereignty principles focused on the concentration of the public digital infrastructure and prevention of offshore data transmission, it became a contractual requirement that the e-NMRA solution be provided within the context of the LGC cloud infrastructure ([ICTA, 2023](#)). The latter, operated and maintained by the Information and Communication Technology Agency (ICTA), refers to a centralized infrastructure cluster providing both Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) service within a secure onshore Tier-3 Data Center environment ([ICTA, 2023](#)). The architecture involved a three-way shared responsibility model:

1. ICTA  
Provided IaaS/PaaS services, and implemented of relevant security measures in compliance with the data backup policies, as stated in the MoUs signed with cloud service users;
2. Epic Lanka  
Acted as a Software-as-a-Service (SaaS) provider, responsible for implementing the application logic, database management, user access control, and fulfilling contractual Service Level

Agreement (SLA) obligations for data protection via regular backups to safeguard against potential disaster, accident or malicious actions;

### 3. NMRA

Represented a data owner with the regulatory powers, responsible for system governance, authorization of access and management of the relationship with Epic Lanka.

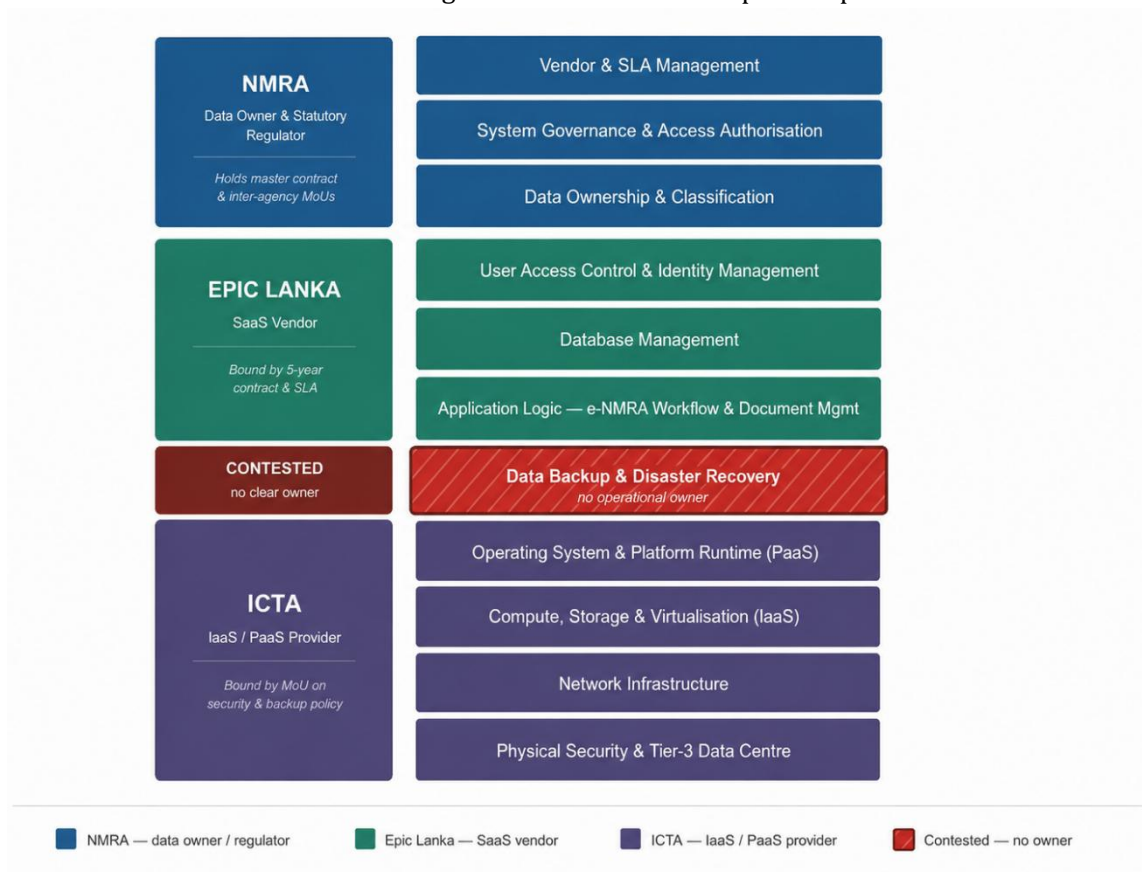


**Figure 1.** Shared responsibility model involving NMRA (data owner), Epic Lanka (SaaS vendor) and ICTA (IaaS/PaaS provider) for the e-NMRA system

### The Deletion Event and Technical Mechanisms

This shared responsibility scheme failed to operate on July 9, 2021, when a former employee of Epic Lanka, an ex-software engineer whose formal resignation had been submitted in advance and whose remaining work time amounted to obligatory six weeks of knowledge transfer activities, performed actions of unauthorized access and deletion of large volumes of vital data (Auditor General's Department, 2021 ; Counterpoint, 2021).

The volume of the deleted material was significant. According to official statements, two terabytes (2,000 GB) of highly classified information was wiped out of the LGC (Auditor General's Department, 2021; Counterpoint, 2021). Specifically, 5,925 individual files, containing the data collected between September 2019 and July 2021, were deleted (Auditor General's Department, 2021; Counterpoint, 2021). As reported, the structural integrity of the primary database of the e-NMRA application, containing the basic text field entries, was still intact. But the deleted files contained huge "attachments" kept on other file servers in the cloud (Counterpoint, 2021).

Those files were crucial for the regulatory process. Namely, they contained sensitive information in the form of proprietary drug formulas, trade secrets provided by foreign pharmaceutical companies, clinical trial data, sample import licenses, and stringent approvals concerning foreign manufacturing facilities. By virtue of the NMRA Act, the institution was under

legal obligation to ensure absolute secrecy regarding this intellectual property. Its deletion endangered all business relationships built between local agencies and foreign pharmaceutical principals, resulting in a complete halt in importing drugs from the global partners into the country (Auditor General's Department, 2021; Parliament of Sri Lanka, 2021).

As the direct consequence of the data breach, the e-NMRA web portal went down with frequent occurrences of "504 Gateway Timeout" error messages and roughly 6,000 pharmaceutical agents' applications, which had been pending at different stages of the approval process, had got stuck in the pipeline (Auditor General's Department, 2023; Counterpoint, 2021). As further investigation demonstrated, absolutely no redundant backups existed in the cloud. Epic Lanka proved unable to perform any of its contractual obligations concerning regular data backups to safeguard its SLAs. There was also no Disaster Recovery System (DRS) configured in the solution (Auditor General's Department, 2021; Auditor General's Department, 2023).

### **Institutional Reactions and Blaming Others**

After the incident, the documentary record shows that responsibility for backup and disaster recovery was disputed among the parties involved. Epic Lanka stated that its role was limited to software development and questioned whether disaster recovery fell within its contractual duties, while ICTA stated that tenant backup was not part of its infrastructure responsibility (Parliament of Sri Lanka, 2021; Counterpoint, 2021). In turn, according to the vendor, LGC infrastructure must have been inherently redundant.

Second, ICTA officials, being responsible for the operation of the LGC infrastructure, insisted that it had never been within their responsibilities to provide tenants with a backup system. And, the agency tried to blame Epic Lanka for the incident (Parliament of Sri Lanka, 2021).

Finally, the NMRA, lacking any internal IT expertise or auditing mechanisms, became fully dependent on the party whose actions put it at risk (Auditor General's Department, 2023). The regulator could resort to nothing but cooperation in the process of forensic analysis of the incident mandated by court order and delayed its provision of hard drives necessary for conducting such activities by the University of Moratuwa and the Criminal Investigation Department (CID) (Parliament of Sri Lanka, 2021 ; Counterpoint, 2021).

### **Geopolitical Context and Weak Governance Scheme**

The timing and circumstances of the data deletion prompted numerous speculations in the public sphere and raised questions during parliamentary debates. First, the event occurred amid the peak of the COVID-19 pandemic, which was characterized by considerable emergency expenses related to public health matters (Parliament of Sri Lanka, 2021).

According to the debates held in the parliament, it was alleged that there was a "pharmaceutical mafia" (Parliament of Sri Lanka, 2021; Parliament of Sri Lanka, 2024). Audit trails enabled by the e-NMRA application threatened some procurement monopolies that could influence drug prices in the country (Parliament of Sri Lanka, 2024; Counterpoint, 2021). During the pandemic, NMRA executives frequently used special procurement pathways and waiver of registration to make purchases from favored providers without undergoing formal approvals (Parliament of Sri Lanka, 2021; Parliament of Sri Lanka, 2024). As later noted by the Deputy Solicitor General in a conversation with the Colombo Chief Magistrate, the wiping out of drug compositions data facilitated this price manipulation strategy (Counterpoint, 2021).

Although it is not possible to definitively prove that the deletion of the information was carried out with a malicious intent, one can argue that the absence of an efficient audit trail along with the lack of a functional backup system allowed for such corruption practices to take place.

### Evaluation Against ISO/IEC 27001 Controls

The NMRA incident illustrates the consequences of deploying advanced technology too far ahead of the organization's GRC maturity. The specific mechanics of governance failure can be determined by aligning the events with established GRC models. ISO/IEC 27001 is the global de facto standard for establishing an ISMS (Malatji, 2023). The normative framework is predicated heavily on its Annex A controls to counteract risks to confidentiality, integrity, and availability of organizational data assets.

**Table 1.** shows the key operational realities of the NMRA mapped against relevant ISO 27001 controls

| ISO 27001 Control Domain | Specific Control Objective                                                                                                                                                             | NMRA / Epic Lanka Operational Reality                                                                                                                                                                      | Consequence of Failure                                                                                                                                          | Evidence source                                                          |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| A.9 Access Control       | A.9.2.6 Removal or adjustment of access rights: access rights of all employees to information processing facilities shall be removed upon termination of their employment or contract. | The software engineer responsible for the deletion had already submitted his resignation but maintained his administrative access to live production file servers during the "knowledge transfer" window.  | Exiting employee and high insider-threat risk actor maintained unrestricted access capabilities to wipe out critical data from a live government database.      | <a href="#">Auditor General's Department (2021); Counterpoint (2021)</a> |
| A.12 Operations Security | A.12.3.1 Information backup: backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.                  | Epic Lanka failed to perform any of its contractual obligations under the SLA in terms of regular data backups. Primary SQL database and attached files were neither backed up nor saved in an independent | Data could not be rolled back using any ordinary IT process. The deletion proved irreversible except via forensic reconstruction of the server hardware itself. | <a href="#">Auditor General's Department (2021, 2023)</a>                |

| ISO 27001<br>Control<br>Domain | Specific Control<br>Objective                                                                                                                                                                                       | NMRA / Epic<br>Lanka<br>Operational<br>Reality                                                                                                                                                                                         | Consequence<br>of Failure                                                                                                                         | Evidence<br>source                                                                                          |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
|                                |                                                                                                                                                                                                                     | secondary<br>location.                                                                                                                                                                                                                 |                                                                                                                                                   |                                                                                                             |
| A.15 Supplier<br>Relationships | A.15.2.1<br>Monitoring and<br>review of supplier<br>services:<br>organizations<br>shall regularly<br>monitor, review<br>and audit supplier<br>service delivery<br>against the agreed<br>security<br>requirements.   | The NMRA<br>lacked both the<br>technical<br>resources and<br>the political will<br>to verify Epic<br>Lanka's SLA<br>claims. ICTA's<br>oversight role<br>vis-a-vis LGC<br>infrastructure<br>went wholly<br>unfulfilled.                 | The total lack<br>of working<br>backups went<br>undetected for<br>years, coming<br>to light only<br>when a<br>disaster made<br>them<br>essential. | <a href="#">Auditor<br/>General's<br/>Department<br/>(2023);<br/>Parliament of<br/>Sri Lanka<br/>(2021)</a> |
| A.17 InfoSec<br>Aspects of BCM | A.17.1.2<br>Implementing<br>information<br>security<br>continuity:<br>establish,<br>document,<br>implement and<br>maintain<br>procedures to<br>maintain<br>information<br>security during<br>adverse<br>situations. | No Disaster<br>Recovery<br>System (DRS)<br>existed prior to<br>the disaster. In<br>February 2021,<br>the plan to<br>implement a<br>DRS had been<br>dropped<br>following board<br>upheavals and<br>mass<br>resignations at<br>the NMRA. | The system<br>suffered<br>extended<br>downtime,<br>severely<br>disrupting<br>critical drug<br>registration<br>efforts during<br>a pandemic.       | <a href="#">Auditor<br/>General's<br/>Department<br/>(2021, 2023)</a>                                       |

Failure to comply with A.15 (Supplier Relationships) were closely associated with the other control gaps. If proper oversight and audits of Epic Lanka had taken place in accordance with ISO 27001 ([Faruq, 2024](#)), the lack of backups (A.12.3) would have been discovered well in advance of the malicious act ([Malatji, 2023](#)). The paper SLA, not verified through evidence-based controls, reflects a low degree of IT GRC maturity.

#### Evaluation Against COBIT 2019 (APO010)

In contrast of ISO 27001, which primarily focuses on fine-grained security controls, COBIT 2019 focuses on governance and alignment of IT with business goals ([ISACA, 2019](#)). Objective APO010: Managed Suppliers of the Align, Plan and Organize (APO) domain aims to reduce risks

associated with poor supplier performance, and to ensure continued value creation from outsourcing (ISACA, 2019; ISACA, 2016).

According to COBIT 2019, organizations cannot outsource their IT governance (ISACA, 2019). Yet the NMRA leadership failed to observe the fundamental precept. It completely entrusted the management of cloud infrastructure to the vendor (Epic Lanka), with no internal verification processes in place. As a result, the official statement released after the disaster was simply that "according to the agreement there has to be a backup" (Parliament of Sri Lanka, 2021; Counterpoint, 2021). That is, there was no IT governance at all, only contractual paper.

COBIT 2019 also dictates clearly demarcated Shared Responsibility Models in cloud computing environments (ISACA, 2016). The tripartite relationship involving the NMRA, Epic Lanka, and ICTA produced a diffuse responsibility chain. ICTA owned and operated the LGC infrastructure. For its part, ICTA assumed data redundancy to be the responsibility of the vendor, the vendor assumed the DRS to be outside its cost budget. Since the NMRA failed to apply COBIT 2019's principles to establish clear ownership over cloud stacks, a huge weakness was created, rendering the data highly susceptible to attack.

### The Design-Reality Gap (ITPOSMO) Analysis

The inability of the NMRA to act during its hour of need is not easily accounted for purely based on technical considerations. To explain the failure to deploy common GRC frameworks in the specific context of a developing country, one must apply Heeks' (2003) "Design-Reality Gap" model (ITPOSMO) (Heeks, 2003; Lessa et al., 2016). Table 2 shows the enormous discrepancies between the idealized design of the e-NMRA system and the reality of Sri Lanka's public sector.

**Table 2.** ITPOSMO Analysis of the e-NMRA Failure.

| ITPOSMO Dimension | System Design Assumption                                                                                                    | NMRA Institutional Reality                                                                                                                 | Impact on Project Failure                                                                                                                                                                  | Evidence source                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Information       | The system assumes that transparency and data centralization in digital format will streamline drug registration worldwide. | Proprietary data containing trade secrets are highly sensitive and valuable, yet centralized without any form of independent safeguarding. | Data centralization without redundancy created a single point of failure. Loss of data jeopardizes relations with foreign manufacturers, putting national pharmaceutical supplies at risk. | Auditor General's Department (2021); Parliament of Sri Lanka (2021) |
| Technology        | Assumes that the "Sovereign" Lanka Government                                                                               | Lack of enforced application-level redundancy and                                                                                          | One single command inside the cloud wiped out 2 TB                                                                                                                                         | Auditor General's Department (2021, 2023)                           |

| <b>ITPOSMO Dimension</b> | <b>System Design Assumption</b>                                                                                            | <b>NMRA Institutional Reality</b>                                                                                                                      | <b>Impact on Project Failure</b>                                                                                                  | <b>Evidence source</b>                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
|                          | Cloud offers built-in enterprise resilience and backup capability.                                                         | independence from SaaS vendor.                                                                                                                         | of both primary and secondary data stores.                                                                                        |                                                     |
| Processes                | Assumes the process to be rational and rule-based, with a digital audit trail in place to ensure transparency.             | COPE audits revealed "special pathways" and workarounds (WORs) employed by NMRA's executives to bypass the committee approvals for major procurements. | System transparency created a powerful incentive for stakeholders to obstruct the transition to the digital process.              | Parliament of Sri Lanka (2021, 2024)                |
| Objectives & Values      | Assumes alignment in NMRA, ICTA, and Epic Lanka towards the shared goal of secure and effective drug registration process. | Self-interest on the part of each stakeholder group produced a fragmented, competing definition of "backup" and DRS.                                   | Misaligned interests translated into contractual ambiguity and insufficient investment in system reliability.                     | Parliament of Sri Lanka (2021); Counterpoint (2021) |
| Staffing & Skills        | Assumes that the NMRA possesses an ICT department capable of managing supplier relationships and verifying SLA compliance. | The NMRA lacks any dedicated ICT skills and technical staffing to verify vendor operations.                                                            | Complete dependency on the vendor resulted in "vendor capture," meaning the NMRA was unable to verify SLA compliance and exercise | Auditor General's Department (2023)                 |

| ITPOSMO Dimension | System Design Assumption                                                                                  | NMRA Institutional Reality                                                                       | Impact on Project Failure                                                                                                   | Evidence source                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                   |                                                                                                           |                                                                                                  | control over backups.                                                                                                       |                                                                                     |
| Management        | Assumes stable institutional leadership with a focus on continuous improvement and risk management.       | The NMRA experienced severe board upheavals and mass resignations in early 2021.                 | Discussion of DRS implementation was disrupted by these political factors and never resumed again until the crisis erupted. | <a href="#">Auditor General's Department (2021); Parliament of Sri Lanka (2021)</a> |
| Other Resources   | Assumes adequate time, funding, and procurement capacity to implement a disaster recovery infrastructure. | Intense fiscal constraints coupled with pandemic-related expenses depleted managerial bandwidth. | DRS provisioning and vendor monitoring became a low priority in the race against deadlines.                                 | <a href="#">Auditor General's Department (2021); Parliament of Sri Lanka (2021)</a> |

A very important insight gained through applying the ITPOSMO model is that, in developing public sectors, technical weaknesses can be reinforced by the very nature of the governing institutions. Delay in implementing the DRS was not due to mere negligence, rather it happened at a time of fierce board infighting and intense pressures to circumvent regular procurement processes amidst a global pandemic. The lack of a functioning digital audit trail and backups enabled continued reliance on old methods and allowed the existing irregularities to flourish without leaving behind digital traces.

### Proposed SCG-VRM Framework

The example of the NMRA makes it clear that simply transplanting existing governance and control frameworks designed for mature economies (such as COBIT 2019 and ISO/IEC 27001 standards) into developing contexts is insufficient ([Rambau et al., 2026](#) ; [Nfuka & Rusu, 2011](#)). These frameworks have merit. There is no doubt that they offer substantial guidelines and best practices concerning governance and security. However, it is implicitly assumed in their design that the institutions have reached a certain level of maturity, that the country has stable political circumstances, strong legal enforcement capabilities, and finally, that there is technical capability within the institution to audit the contractor's work. None of these assumptions are often valid in developing countries ([Rambau et al., 2026](#) ; [Nfuka & Rusu, 2011](#)). As Heeks suggests, there is a major reason behind it – the ITPOSMO framework explains why developed countries tend to export their frameworks but often ignore their design reality gaps ([Heeks, 2003](#) ; [Lessa et al., 2016](#)).

To address the earlier mentioned problems, the Sovereign Cloud Governance and Vendor Risk Management model (SCG-VRM) was conceived. The SCG-VRM localizes existing GRC principles to the context of the sovereign cloud operation in developing countries, combining three critical features: mandated digital sovereignty, automated compliance checking, and hybrid redundancy of operations. The novelty of the model does not lie in developing brand-new technical controls. Zero Trust architecture, CSPM technology, air-gapping backups, and Shared Responsibility Models are already known cybersecurity best practices (ISACA, 2019 ; Malatji, 2023 ; Boyens et al., 2022 ; Gupta et al., 2024). What this model contributes to the field is an understanding of how to contextualize these technologies in the local setting of developing public sectors, taking into account low institutional enforcement capability, vendor capture tendencies, and other peculiarities of emerging digital economies. SCG-VRM accounts for Heeks' Design-Reality Gaps that make the imported GRC frameworks ineffective in emerging countries (Heeks, 2003 ; Lessa et al., 2016 ; Nfuka & Rusu, 2011).



**Figure 2.** Integration concept of the SCG-VRM

The SCG-VRM model should be seen as a target state that will require institutional capacity building efforts to reach, rather than something that should be achieved immediately. There are four core components of SCG-VRM.

The following Table 3 makes the derivation of the proposed model explicit. Each pillar is linked to a documented weakness identified in the case and to the governance problem that the proposed response is intended to address. The transition from the case findings to SCG-VRM follows a problem-to-response logic, and the mapping should be understood as a conceptual inference rather than an empirically validated causal relationship. The ISO/IEC 27001 analysis identifies weaknesses in access control, backup, supplier monitoring, and continuity. The COBIT analysis identifies weaknesses in accountability and shared responsibility. The ITPOSMO analysis indicates how institutional capacity, management instability, resource constraints, and process conditions shaped the context in which these controls were implemented and verified. Taken together, these findings indicate four recurring governance problems: dependence on a single recovery environment, insufficient continuous verification of vendors, ambiguity in responsibility allocation, and limited institutional capacity for independent enforcement. SCG-VRM translates these four problems into four corresponding governance responses.

**Table 3.** Weaknesses mapped to SCG-VRM response

| Documented weakness                                          | Interpretation from the case                             | SCG-VRM response                             |
|--------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------|
| No effective redundant backup / no functioning DRS           | A single deletion could become effectively irreversible. | Mandated hybrid sovereign redundancy.        |
| Privileged access remained during vendor offboarding; vendor | Contractual controls were not enough without ongoing     | Continuous automated vendor risk management. |

| Documented weakness                                                           | Interpretation from the case                                                       | SCG-VRM response                             |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------|----------------------------------------------|
| obligations were not independently verified                                   | verification.                                                                      |                                              |
| NMRA, Epic Lanka, and ICTA gave different accounts of recovery responsibility | Recovery responsibility was not sufficiently clear or verifiable.                  | Codified shared responsibility arrangements. |
| Limited internal technical and audit capacity                                 | The organisation had limited ability to verify vendor claims and enforce controls. | Sovereign enforcement and capacity building. |

#### *Pillar 1: Mandated Hybrid Sovereign Redundancy*

It became clear in the NMRA case that even having a sovereign cloud (i.e., the LGC) where national records are stored is pointless if the vendor is allowed unrestricted administrative privileges to control both the main database and the backup environment (Floridi, 2020 ; ICTA, 2023). Digital sovereignty must include operational resilience as well. The SCG-VRM model, accordingly, requires mandatory hybrid redundancy.

##### *a. Air-Gapped State Controlled Backup Environment*

In the case of sovereign clouds in emerging nations, for example, the NMRA may outsource the SaaS application but must still mandate automated backup of the data daily into an offline (air-gapped) database controlled by the state agency. And such backups must be separate and inaccessible from the primary environment (e.g., cloud).

##### *b. Administrative Privilege Separation*

Vendors may be contractually and technologically precluded from having any access whatsoever to the secondary database. It should be kept in mind that if a vendor can remotely connect to and access the secondary database, then a misbehaving vendor employee or a ransomware attack may completely destroy the data.

#### *Pillar 2: Continuous Automated Vendor Risk Management*

Traditional approaches to VRM rely on static questionnaires and periodic audits to assess vendor compliance – an approach that proved entirely ineffective in the NMRA case (Faruq, 2024 ; AlGhamdi et al., 2020). The SCG-VRM requires transitioning to a much stricter Continuous Automated Compliance.

##### *a. Vendor API-Driven Telemetry*

State IT organizations (e.g., ICTA) should install Cloud Security Posture Management tools that monitor vendor compliance with SLAs in real time. These tools should collect vendor's telemetry via its API and check compliance with relevant standards.

##### *b. Zero Trust Architectural Principles*

Public sector cloud contracts should mandate ZTA. Vendors must ensure that any access is made according to the least privileged identity-based model, with Just-In-Time access control being applied as widely as possible. In particular, the risky practice of granting vendor personnel persistent access rights to the cloud during the knowledge transfer period must be banned.

#### *Pillar 3: Codified and Legally Binding SRMs*

Diffusion of responsibilities between the NMRA, Epic Lanka, and ICTA was the key issue in the case, making the NMRA unable to act quickly in accordance with its vendor responsibilities. The third pillar of the SCG-VRM model is thus the requirement for codified and binding Shared

Responsibility Matrices (SRMs) ([ISACA, 2019](#) ; [ISACA, 2016](#)).

a. Explicit SRM Mapping

Every document concerning procurement of services should specify, in detail, who is responsible for the management of IaaS, SaaS, data encryption, database backup and disaster recovery. Ambiguity in SRM should be legally construed as a violation of contract terms.

b. SLA Requirements and Penalties

Contracts with the vendor must contain SLAs and penalties that should apply immediately in the case of the former's breach. RTO and RPO metrics should be specified in advance along with strict penalties associated with their breach.

*Pillar 4: Sovereign Enforcement and Capacity Building*

Without the ability to enforce the rules and monitor vendor compliance, any technical GRC framework is bound to fail. SCG-VRM accordingly incorporates ITGO principles to address design-reality gaps by explicitly considering the soft side of IT governance ([Heeks, 2003](#) ; [Nfuka & Rusu, 2011](#)).

a. Mandatory State Internal IT Hubs

Any public institution working with critical data (e.g., NMRA) must create an independent internal IT hub capable of interpreting and enforcing SLAs. Governments can never rely entirely on the vendor – they need to have their own auditing capability for independent interpretation of logs.

b. Legislative Changes and Categorization

Domestic data protection laws must explicitly categorize health, pharmaceutical, and citizens' personal data as Critical National Information Infrastructure ([ICTA, 2023](#)). Malicious vendor behavior, including sabotage or obfuscation, must be met with stiff penalties. In addition, parliamentary oversight committees (e.g., COPE) should be regularly informed about IT governance in the nation by annual reports. Given that developing nations often lack either technological or financial resources needed to implement a full-fledged GRC framework ([Nfuka & Rusu, 2011](#)), the SCG-VRM must be seen as a target state achieved through phased capacity-building, rather than one-shot solution. To overcome the gap in feasibility, developing nations could seek support from various international digital development programs offered by World Bank and other institutions ([World Bank, 2022](#)).

## CONCLUSIONS

The findings address the three objectives of the study. First, consistent with Objective 1, the documentary evidence identifies weaknesses in privileged-access management, backup and disaster-recovery arrangements, vendor oversight, responsibility allocation, and internal technical capacity within the NMRA cloud environment. These findings are supported primarily by statutory audit and parliamentary records, with supplementary technical reconstruction from cybersecurity reporting. For Objective 2, the ISO/IEC 27001, COBIT 2019, and ITPOSMO analyses indicate that the documented weaknesses were not limited to individual technical controls. They also reflected weaknesses in supplier oversight, shared responsibility, institutional capability, management continuity, and the ability to verify contractual requirements. The analysis therefore suggests a gap between formal governance requirements and the institutional capacity available to implement and enforce them. As for Objective 3, the study derives the SCG-VRM model as a conceptual governance response to these identified weaknesses. Its four pillars mandated hybrid sovereign redundancy, continuous automated vendor risk management, codified shared responsibility arrangements, and sovereign enforcement and capacity building are mapped explicitly to documented case

weaknesses in Table 3. The model is not presented as an empirically validated solution, but as a context-sensitive conceptual model requiring further empirical testing.

The findings should nevertheless be interpreted within the limitations of the study. The analysis is based on secondary documentary evidence concerning a single public-sector case in Sri Lanka. Consequently, the findings should not be generalised statistically to all developing countries or all sovereign cloud environments. Similarly, the proposed SCG-VRM framework represents a theoretically derived model based on the identified case conditions and established literature; its effectiveness has not yet been tested through implementation or comparative empirical studies. These limitations provide opportunities for future research to examine the framework across multiple public-sector cloud environments and to empirically evaluate whether its proposed controls improve vendor accountability, operational sovereignty, and data resilience.

Overall, the study demonstrates that the governance of public-sector cloud infrastructure cannot be evaluated solely by examining technical security controls or the physical location of government data. The NMRA case suggests that effective governance also depends on the allocation of responsibility among government agencies and vendors, the continuous verification of vendor obligations, the independence of recovery mechanisms, and the institutional capacity to exercise oversight. The SCG-VRM framework brings these dimensions together and provides a context-sensitive foundation for further research into sovereign cloud governance and vendor risk management in developing digital economies.

#### **LIMITATION & FURTHER RESEARCH**

This study is based on a single case of public sector cloud governance failure (NMRA incident). Generalizability is limited. Although this offers useful insight into IT governance problems in a developing nation, it may reflect very specific economic and political conditions of Sri Lanka in 2021. The SCG-VRM framework is purely theoretical at the moment, and further practical testing is necessary to evaluate its efficacy.

Future research could involve cross-country comparisons of IT governance problems in public sectors of developing nations (i.e., Sub-Saharan Africa, Southeast Asia, Latin America) and test the SCG-VRM hypotheses on different institutional backgrounds. Quantitative analysis of air-gapped sovereign backups' cost-benefit ratio vs. hyperscaler-native redundancy could help developing governments decide which strategy should be implemented.

The study relies exclusively on secondary documentary evidence, including statutory audit reports, parliamentary proceedings, media investigations, cybersecurity publications, and existing academic and governance literature. Although triangulation across these sources provides multiple perspectives on the NMRA incident, secondary evidence cannot fully substitute for direct access to the individuals, systems, and organisational processes involved in the event. Consequently, some interpretations presented in this study remain dependent on the completeness, accuracy, and perspective of the available documentary records.

#### **REFERENCES**

- Al-Ansari, A. O., & Alsubait, T. M. (2022). Predicting cyber threats using machine learning for improving cyber supply chain security. In *2022 National Computing Colleges Conference (NCCC)* (pp. 123–130). IEEE. <https://doi.org/10.1109/NCCC57165.2022.10067692>
- AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, 99, Article 102030. <https://doi.org/10.1016/j.cose.2020.102030>
- Alharbi, F., Sabra, M. N. A., Alharbe, N., & Almajed, A. A. (2022). Towards a strategic IT GRC framework for healthcare organizations. *International Journal of Advanced Computer*

- Science and Applications*, 13(1). <https://doi.org/10.14569/ijacsa.2022.0130125>
- Auditor General's Department. (2021). *Report of the Auditor General on the financial statements of the National Medicines Regulatory Authority for the year ended 31 December 2021*. National Audit Office, Sri Lanka. [https://www.naosl.gov.lk/web/images/audit-reports/upload/2021/state\\_corporation/2-xiii/National-Medicines-Regulatory-E.pdf](https://www.naosl.gov.lk/web/images/audit-reports/upload/2021/state_corporation/2-xiii/National-Medicines-Regulatory-E.pdf)
- Auditor General's Department. (2023). *Report of the Auditor General on the financial statements of the National Medicines Regulatory Authority for the year ended 31 December 2023*. National Audit Office, Sri Lanka. <http://www.auditorgeneral.gov.lk/web/images/audit-reports/upload/2023/State-Corporations/2-XXIII/National-Medicines-Regulatory-Authority---e.pdf>
- Bena, Y. A., Ibrahim, R., Mahmood, J., Talpur, N., Nasser, M., Ayemowa, M. O., & Yusuf, M. N. (2024). Harnessing and mitigating big data governance challenges using hybrid approach: A systematic literature review. *IEEE Access*, 12, 175151–175175. <https://doi.org/10.1109/ACCESS.2024.3498947>
- 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 800-161r1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-161r1>
- Cloud Security Alliance. (2024). *Information technology governance, risk, and compliance in healthcare* (Version 2). <https://cloudsecurityalliance.org/artifacts/information-technology-governance-risk-and-compliance-in-healthcare-v2>
- Counterpoint. (2021). *Deletion of data in the NMRA: Human error or a scam?* Counterpoint Investigative Reporting. <https://counterpoint.lk/deletion-data-nmra-human-error-scam/>
- Debreceeny, R. S., & Gray, G. L. (2009). IT governance and process maturity: A field study. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1–10). IEEE. <https://doi.org/10.1109/HICSS.2009.278>
- Faruq, M. O. (2024). Vendor risk management in cloud-centric architectures: A systematic review of SOC 2, FedRAMP, and ISO 27001 practices. *International Journal of Business Ecosystem & Strategy*, 4(1), 1–32. <https://doi.org/10.63125/j64vb122>
- Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-2>
- Gupta, D., Elluri, L., Jain, A., Moni, S. S., & Aslan, O. (2024). Blockchain-enhanced framework for secure third-party vendor risk management and vigilant security controls. In *2024 IEEE International Conference on Big Data (BigData)* (pp. 5577–5584). IEEE. <https://doi.org/10.1109/BigData62323.2024.10825025>
- Heeks, R. (2003). *Most eGovernment-for-development projects fail: How can risks be reduced?* (iGovernment Working Paper Series). University of Manchester. <https://gsdrc.org/document-library/causes-of-e-government-success-and-failure-design-reality-gap-model/>
- Heeks, R. (2006). Health information systems: Failure, success and improvisation. *International Journal of Medical Informatics*, 75(2), 125–137. <https://doi.org/10.1016/j.ijmedinf.2005.07.024>
- Information and Communication Technology Agency of Sri Lanka. (2023). *Sovereign cloud strategy Sri Lanka v0.4*. <https://www.icta.lk/icta-assets/uploads/2023/11/sovereign-cloud-strategy-sri-lanka-v0-4.pdf>
- Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet*, 4(3–4), 40–71. <https://ideas.repec.org/p/zbw/itse11/52197.html>

- ISACA. (2016). *Vendor management: Using COBIT 5*.
- ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*.
- Leka, E. (2024). *Exploring digital sovereignty through data flows: Empirical evidence from the backbone of the internet* [Conference presentation]. Toulouse School of Economics Postal Economics Conference / Institut Mines-Télécom Business School. <https://www.tse-fr.eu/sites/default/files/TSE/documents/conf/2026/postal/leka.pdf>
- Lessa, L., Negash, S., & Belachew, M. (2016). Steering e-government projects from failure to success: Using design-reality gap analysis as a mid-implementation assessment tool. *Electronic Journal of Information Systems in Developing Countries*. [https://www.researchgate.net/publication/305356511\\_Steering\\_E-Government\\_Projects\\_from\\_Failure\\_to\\_Success\\_Using\\_Design-Reality\\_Gap\\_Analysis\\_as\\_a\\_Mid-Implementation\\_Assessment\\_Tool](https://www.researchgate.net/publication/305356511_Steering_E-Government_Projects_from_Failure_to_Success_Using_Design-Reality_Gap_Analysis_as_a_Mid-Implementation_Assessment_Tool)
- Makumbani, H., & Tsibolane, P. (2025). Design-reality gap analysis of health information systems failure. *Procedia Computer Science*, 256, 949–956. <https://doi.org/10.1016/j.procs.2025.02.199>
- Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. In *2023 International Conference on Cyber Management and Engineering (CyMaEn)* (pp. 117–122). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10051114>
- Mitchell, A. D., & Samlidis, T. (2021). Cloud services and government digital sovereignty in Australia and beyond. *International Journal of Law and Information Technology*, 29(4), 364–394. <https://doi.org/10.1093/ijlit/eaac003>
- Nfuka, E. N., & Rusu, L. (2011). The effect of critical success factors on IT governance performance in public sector organizations in a developing country. *Industrial Management & Data Systems*, 111(9), 1418–1448. <https://doi.org/10.1108/02635571111182773>
- Parliament of Sri Lanka. (2021). *COPE objects to the unconstitutional decision taken by the Board of Directors of the National Medicines Regulatory Authority (NMRA)*. <https://www.parliament.lk/en/home/parliament-news/view/3574>
- Parliament of Sri Lanka. (2024). *COPE sub-committee to examine the National Medicines Regulatory Authority. Committee on Public Enterprises*. <https://www.parliament.lk/en/home/parliament-news/view/4452>
- Rambau, T. M., Munyoka, W., Phahlamohlaka, L. J., & Kadyamatimba, A. (2026). Evaluating cyber resilience frameworks for e-government: Applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in developing country contexts. *Information and Computer Security*. <https://doi.org/10.1108/ICS-09-2025-0376>
- Tamilarasi, R., Santhosh Kumar, P. N., Ghantasala, G. S. P., & Garg, S. (2024). Machine learning challenges of e-government models of cloud computing in developing countries. In *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE. <https://ieeexplore.ieee.org/document/10498915>
- World Bank. (2022). *Government migration to cloud ecosystems: Multiple options, significant benefits, manageable risks*. <https://openknowledge.worldbank.org/items/7baff007-7bb9-4623-b229-b105cbf47284>