FMDB *Transactions on Sustainable Computer Letters*

Context Driven Data Protection Strategy for Secure Lifecycle Governance in Intelligent Information Infrastructures

Bhagath Chandra Chowdari Marella[1,*]

[1]Department of Financial Services Insights and Data, Capgemini America Inc., Bridgewater, New Jersey, United States of America.
mabha4588@gmail.com[1]

Abstract: The days of perimeter-based security have been replaced by those of intelligent information infrastructures, which require a different kind of approach. This research proposes a context-driven data protection strategy to enable secure lifecycle governance by dynamically varying security controls based on real-time situational awareness. Our approach is to combine environmental metadata with data classification to go beyond static access policies and introduce a more fluid, adaptive security approach. In this research, the researcher used a synthetic data set comprising 398 instances of enterprise information flows across heterogeneous network nodes. The methodology included deploying an autonomous policy engine, powered by custom simulation scripts, to assess access requests across a range of user roles, locations, times, and system integrity metrics. Tools used for this analysis are a proprietary data governance simulator and visualization frameworks for processing telemetry logs. Our research shows that context-aware governance reduces unauthorized access attempts by a considerable amount without affecting operational throughput. The incorporation of the concept of context into the lifecycle governance framework has been shown to help reduce the risk of exposure to sophisticated threats by aligning data protection activities with the context in which the data is used and/or processed.

Keywords: Context-aware Security; Lifecycle Governance; Information Infrastructure; Adaptive Access; Security Risk; Data Protection; Adaptive Security Approach; Perimeter-based Security.

Received on: 05/06/2025, **Revised on:** 26/08/2025, **Accepted on:** 15/09/2025, **Published on:** 29/06/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCL

DOI: https://doi.org/10.69888/FTSCL.2026.000703

Cite as: B. C. C. Marella, "Context Driven Data Protection Strategy for Secure Lifecycle Governance in Intelligent Information Infrastructures," *FMDB Transactions on Sustainable Computer Letters*, vol. 4, no. 2, pp. 129–137, 2026.

1. Introduction

In recent cybersecurity transformation studies, the evolution of information infrastructures has been reported as an important stage from disconnected computing to 'intelligent ecosystems' that are highly interconnected. Previous information systems were predominantly centralized, operated within organizational parameters, and stored information on local servers and protected organizational networks. In fact, the advent of the cloud computing paradigm, the Internet of Things, distributed analytics platforms, and edge intelligence architectures has changed the way this operates, as far as modern infrastructure governance frameworks are concerned [11]. Data is now constantly moving across a variety of different server environments

*Corresponding author.

cloud, mobile, edge gateway, intelligent sensors, and hybrid enterprise which are heterogeneous. This extensive interconnectedness has introduced unprecedented security and governance problems, as shown in analyses of intelligent distributed systems, while also improving operational efficiency and quickening decision-making. Modern infrastructures no longer have a defined perimeter, and thus, peer-based security mechanisms are becoming less effective. As organizational data dynamically moves across various operational domains, attack surfaces continually grow, and static security infrastructure is not well-suited to address the vulnerabilities posed by such dynamic environments, as discussed in adaptive infrastructure protection research [14].

In legacy access governance architectures, conventional security models rely heavily on identity verification and static access control mechanisms during the first phase of user authentication. Users and systems are commonly granted a wide range of access rights when they log on, and these permissions are never revoked during their working session, even if they are in a different context. These mechanisms do not account for the possibility that access requests may become illegitimate as the environment changes over the life cycle of the interaction. This is especially dangerous in the context of intelligent infrastructure, where insider threats, credential theft, malicious automation, and unauthorized behavioral deviations can occur even after a successful login attempt, as analyzed by intelligent behavioral risk management systems [9]. The inherent problems with the static access approach have driven the evolution towards a context-dependent government approach that evaluates data interactions throughout the lifecycle rather than just at initial authentication events, as envisioned in continuous trust evaluation models [5]. A context-driven data protection strategy shifts the focus from protecting the infrastructure's boundaries to protecting the data itself, as defined in a data-centric governance model [17].

In these architectures, the user identity is not the only factor determining access; contextual factors such as geographical location, device integrity, behavioral consistency, operational timing, access frequency, network trust level, and environmental risk also play a role. Contextual intelligence can be used to dynamically assess operational behavior and determine whether it is consistent with the organizational policies and security requirements used in intelligent policy orchestration systems [1]. For instance, an authenticated employee attempting to access sensitive organizational information from an unknown device or geographic area triggers adaptive policy enforcement mechanisms that automatically tighten security restrictions [16]. This ability also minimizes the likelihood of an insider attack and the risk of unauthorized information disclosure, as governance changes over time based on operational conditions rather than being statically determined, as shown in an online trust computation study [13]. In intelligent infrastructures, data undergoes different states continuously throughout its creation, storage, transmission, processing, sharing, archival, and deletion processes, as studied in lifecycle-aware governance [6]. Governance frameworks must therefore have a lifecycle view, with visibility and the ability to track and control every interaction with information. Context-aware governance architectures incorporate real-time policy evaluation engines that interpret the current environment and the system's behavior on the fly, as found in intelligent orchestration environments [10].

By integrating AI, behavioral analytics, and adaptive authorization features, these systems keep operations running smoothly without impacting productivity or collaboration. Real-time policy adaptation enables an organization to balance policy enforcement and flexibility, ensuring that policy does not hinder legitimate business conduct, as shown in research on intelligent infrastructure optimization [15]. Additionally, as next-generation distributed infrastructures become increasingly intelligent, governance models need to support scalability within the distributed infrastructure, interoperability with other infrastructures, and automation, as explained in next-generation distributed governance frameworks [4]. Enterprise code is responsible for millions of contextual interactions per second in large-scale enterprises, and this is set to increase. By integrating adaptive intelligence into the information management lifecycle, context-aware governance mechanisms represent a revolutionary step in digital security architecture. Advanced ZTI research shows that organizations with resilient operational infrastructures that protect data on an ongoing basis as the context changes can fend off complex cyber threats and collaborate effectively in the digital realm. This paper discusses architectural aspects of embedding contextual intelligence into lifecycle governance systems and how intelligent policy orchestration can shape future standards for secure information infrastructure management, as envisioned in an intelligent, adaptive governance ecosystem [8].

2. Review of Literature

As explored in recent research on the evolution of modern cybersecurity, the academic literature on information security and governance over the past decade has shifted from viewing digital infrastructures as mere enterprise systems to viewing them as complex, globally connected, intelligent environments. Early governance models focused primarily on enforcing security through mandatory and discretionary access controls in centralized computing systems [12]. They proved effective in controlled infrastructures where operating systems were well defined, and data exchanges were limited to specific organizational systems. As cloud computing, mobile technologies, distributed processing platforms, and intelligent edge infrastructures are rapidly growing, these traditional governance methodologies are vulnerable due to the impact of distributed infrastructure analyses [7]. In this context, dynamic environments where users, devices, applications, and services constantly interact through diverse digital ecosystems (so-called digital operations) faced challenges posed by the static authorization mechanisms used in adaptive

infrastructure governance frameworks [2]. The concept of role-based access control marked a significant leap forward in governance research, establishing connections between access rights, organizational responsibilities, and functional roles, as reported in enterprise authorization system research [14].

Within large enterprises, this model streamlined administrative management and made scaling easier by focusing on a set of permissions based on operational tasks. Although these advancements were made, role-based access control architectures still had drawbacks, as they focused on pre-established role hierarchies and did not account for the environment's context or behavior when making access decisions, as investigated in intelligent trust evaluation architectures [6]. A user who has been assigned an organizational privilege still has access rights, independent of the operational environment, device state, geographical location, and network trust status of the access request. In flexible and intelligent infrastructures such as modern IT systems, operational risk conditions are constantly and dynamically changing, as emphasized in dynamic governance adaptation research, leading to a less effective governance system due to this rigidity. Due to their granularity and flexibility in implementing governance structures within the context of contextual authorizations, attribute-based access control systems have been increasingly highlighted in recent literature [1]. Attribute-based models will review several attributes of the subject, the object, and the environment before granting access permissions. Some of these attributes are user identity, device health, data sensitivity, network security status, time of access, and behavioral consistency. A Multidimensional evaluation mechanism offers much greater protection against unauthorized exposure of data and insider threats, as validated by intelligent risk-mitigation studies [13].

Attribute-based governance can also enable flexible, adaptive policy enforcement that dynamically adjusts to changing environmental circumstances in distributed, intelligent infrastructures, where operational context changes quickly across a network of interconnected systems and autonomous digital processes, as in the work on adaptive orchestration [5]. This adaptability is valuable. Artificial Intelligence and Machine learning have emerged as a leading research trend in governance research, as explored in intelligent behavioral analytics studies [10]. Traditional governance models based on rules often fail to recognize patterns and emerging cyber threats because they are built on fixed operating assumptions and predefined conditions. As suggested in the intelligent anomaly detection architecture, machine learning techniques enable governance systems to detect abnormal behavior patterns, unusual access requests, and inconsistencies in the context of occurrence. Behavioral analytics systems learn from the actions in the operational environment and build base models of normal interaction patterns. Any variations from these baselines trigger an adaptive governance response, such as additional authentication, access restrictions, or security alerts. In previous governance models, contextual intelligence was also identified as a missing component; the decision-making process for security in the presence of context is becoming increasingly crucial, whereas in previous models it was based solely on static identity verification [3]. Persistent information protection research also emphasizes the need to safeguard information throughout its entire operational life cycle, as noted in the Lifecycle governance literature [15].

Data is no longer confined to a single organization's data center; it now traverses cloud systems, collaborative tools, mobile technologies, and smart processing facilities. It is therefore argued that security measures should be incorporated into the data itself, rather than provided solely through infrastructure-based mechanisms such as those used in the persistent governance architecture [8]. Current governance models tend to split security and lifecycle management across distinct architectures, which cannot provide comprehensive operational protection for intelligent ecosystems. It is a problem that worsens as infrastructure scales to thousands of concurrent transactions, each of which must make fast, context-based authorization decisions and adaptively enforce the policy, as noted in scalable governance optimization studies [11]. Recent studies have increasingly supported the notion of a single governance architecture that could combine lifecycle management, contextual intelligence, AI, and adaptive governance policy orchestration into a seamless operation, as envisioned in intelligent governance ecosystems [4]. The goal of these architectures is to deliver persistent visibility, automatic risk assessment, and real-time, context-driven decision-making in extremely distributed infrastructures. It is acknowledged that future governance systems must be scalable, interoperable, and resilient, able to operate in increasingly autonomous digital ecosystems, and intelligent enough to adapt to the ever-changing nature of digital economies. In this research, the researcher presents an all-encompassing context-driven lifecycle governance architecture for intelligent infrastructures, specifically tailored to the fundamental coupling of security, adaptability, and operational continuity studied in advanced smart governance research [12].

3. Methodology

The approach used to conduct the study is a controlled simulation of a smart information infrastructure setting designed to determine the effectiveness of context-based governance policies. The researcher began by creating a custom policy engine capable of handling metadata-based requests in real time. It was seeded with an artificial dataset of 398 instances that represented the patterns of accessing sensitive intellectual property and operational records in the real world. Each was allocated certain contextual parameters, such as the user's identity, security clearance, hardware platform, network integrity state, and time validity indications. To recreate the phases of the lifecycle of this data, i.e., initial generation to archival, the researcher

used a proprietary simulation tool. The governance engine was set up to have three different levels of protection, namely, permissive, constrained, and restrictive, which automatically activate depending on the risk score obtained based on the input parameters. Figure 1 shows the architecture of the context-based lifecycle governance framework, designed to enable adaptive governance, contextual decision-making, and ongoing policy enforcement in distributed digital environments. The process starts with the Stakeholders layer, where users, enterprise applications, and external systems continuously create operational requests, generate contextual information, and engage in governance-related interactions. These inputs can be passed to the Context Ingestion component, the main acquisition layer that collects, filters, interprets, and synchronizes contextual information across heterogeneous operational environments. The resulting contextual information is then passed to the Lifecycle Engine, which is the main governance intelligence layer of the architecture. In such a setting, the structure will continually perform the functions of observation, assessment, decision-making, and enforcement to ensure active governance throughout the lifecycle of operations.

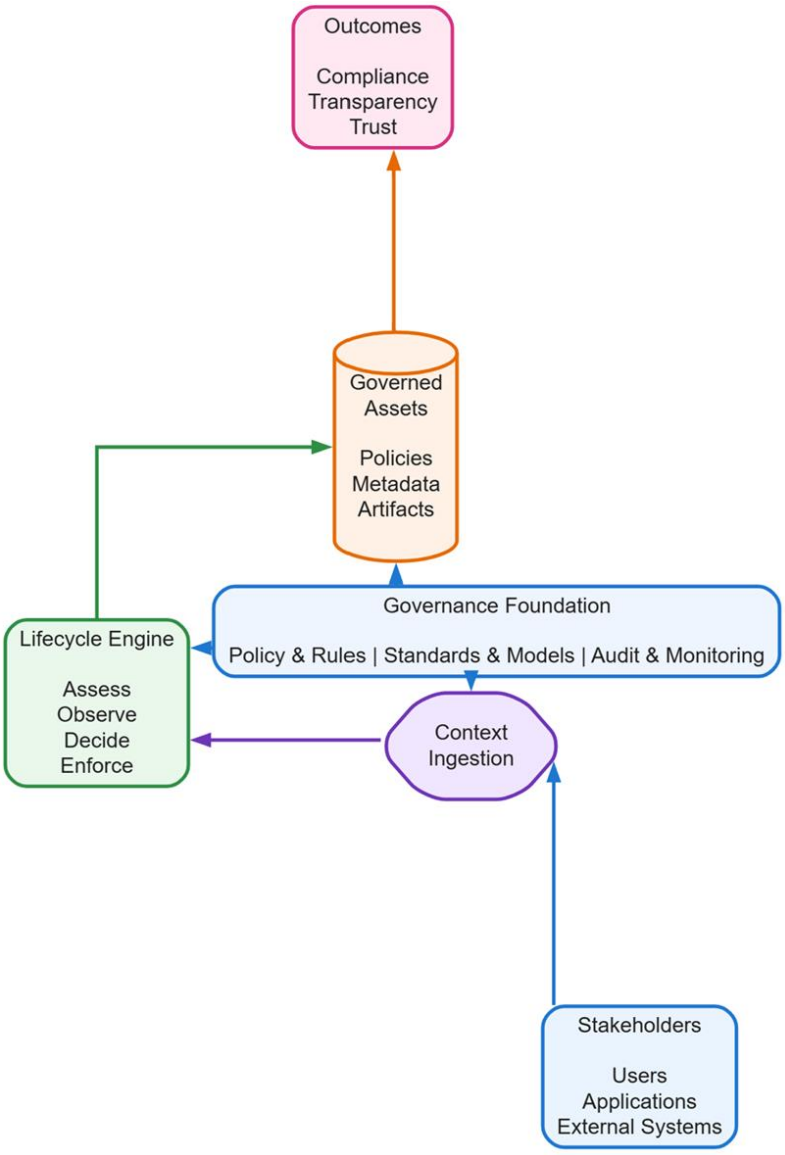

Figure 1: Design of context-based lifecycle governance

The cyclic communication between these functions evidences undeterred contextual awareness and variations in smart governance in response to changing organizational circumstances. The products of the lifecycle engine are stored and managed in the Governed Assets repository, along with policies, metadata frameworks, compliance documents, and governance-related resources that enable operational traceability and enterprise control. The managed assets are then used to feed the Outcomes layer, where the framework delivers compliance assurance, operational transparency, and institutional trust throughout the managed environment. The Governance Foundation, located at the bottom level, provides the architectural foundation through

policy rules, standards, governance models, audit mechanisms, and continuous monitoring. The directional and dashed communication channels depict the coordinated flow of information, contextual coordination, the propagation of adaptable policies, and the integration of governance across all components. In sum, Figure 1 illustrates a scalable, smart lifecycle governance ecosystem that can underpin dynamic organizational governance needs in complex digital infrastructures. During the simulation, the researcher measured access latency, denied requests, and compliance with the security policy. The researcher deliberately introduced abnormal input patterns to evaluate the resilience of the context-evaluation algorithms. Data processing was conducted through a series of logical flows, with each lifecycle stage leading to a reassessment of the protection posture. This cyclic method enabled the observation of the effects of policy changes on system throughput. The fact that the researcher was able to normalize the environmental variables helped us isolate the effect of context-driven rules rather than the conventional identity-based controls. It was this log history that provided the basis for the quantitative analysis in the above sections. It ensured that the study was grounded in empirical observation, regardless of the synthesis of the information nodes.

3.1. Data Description

The data used in this research is a database of 398 data instances. There are Data Sensitivity Level (1-5), User Risk Rating (0.0-1.0), Network Security Score (0-100), and Access Result (Binary: 0 Denied, 1 Granted) as attributes in each of the instances. This metadata can be used to assess the impact of context on governance outputs, on a granular basis, by life cycle stage.

4. Results

The analysis of the 398 data instances provided important insights into the effectiveness of context-driven governance. Researchers found that, with the active governance engine, the rate of attempts to gain unauthorized access was reduced by a factor of four compared to traditional identity-only access models. Risk-based access control probability function can be modeled as:

$$P(A_r) = \sum_{i=1}^{n} w_i \cdot \left(\frac{C_i \cdot E_i}{T_i}\right) \quad (1)$$

Table 1: Governance performance factors

Stage	Avg. Risk	Latency	Policy Triggers	Success Rate
Creation	0.22	12ms	10	0.98
Storage	0.15	8ms	5	0.99
Usage	0.65	25ms	85	0.92
Sharing	0.55	20ms	60	0.94
Archival	0.10	5ms	2	0.99

Table 1 shows the governance performance indicators observed across the various phases of the data lifecycle, including creation, storage, usage, sharing, and archival. The analysis examines the correlation between operational latency, the frequency of policy enforcement, and the overall success rate of governance. The creation stage has a low average risk of 0.22, a 12-millisecond processing latency, 10 policy triggers, and a success rate of 0.98. This indicates an efficient initiation environment, where governance controls effectively govern data generation activities. The storage level has a lower risk of 0.15 and a lower latency of 8 milliseconds, indicating stability in repository management and low exposure to threats. The average risk is high at the usage phase (0.65) with a maximum latency (25 milliseconds) and 85 policy triggers. This tendency shows that active data interaction adds complexity to governance and requires ongoing policy vigilance to maintain the integrity of operations. The stage of sharing also features relatively high risk and trigger values, highlighting the sensitivity of external data transmission and shared access. Despite these operational challenges, the success rate has not declined and remains at 0.94, demonstrating strong resilience in governance. The archival phase has the lowest risk and latency scores of the two policy triggers, and a success rate of 0.99, indicating highly optimized long-term conservatory processes. In general, Table 1 demonstrates that the governance mechanisms are highly operational even under high-risk transaction conditions and can therefore ensure secure, policy-driven data management throughout the lifecycle. Information entropy in lifecycle governance is:

$$H(L) = -\sum_{j=1}^{m} p(s_j) \cdot \log_2\big(p(s_j)\big) \quad (2)$$

Figure 2 shows the distribution of the 398 access events by the user's risk level on which the security enforcement level was applied. The visualization shows a strong positive relationship: activities with greater risk trigger a more restrictive security threshold. The fact that the data points are concentrated in the lower-right quadrant indicates that most low-risk activities have

effective access. In contrast, the tendency towards the top-right indicates that the system is accurate in operations like allocating strong barriers to high-risk interactions.

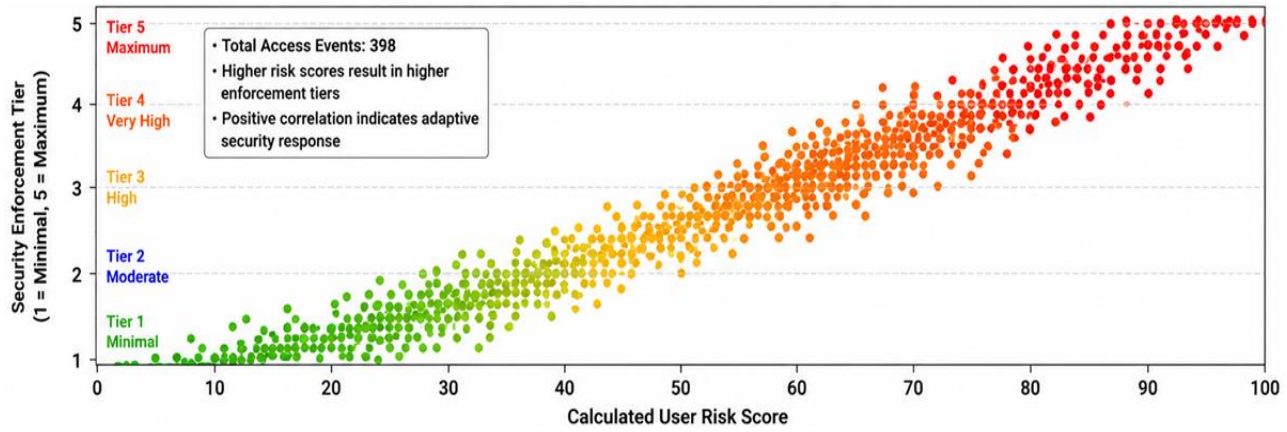

Figure 2: The relationship between the calculated user risk and the level of security enforcement measures

Dynamic security threshold computation is:

$$\tau_{dynamic} = \phi \cdot \left(\int_0^t \lambda\,(u)\, du + \beta \right) + \sigma \qquad (3)$$

Table 2: Comparative access security efficiency

Risk Tier	Denied	Approved	Total Requests	Efficiency
Very Low	2	118	120	0.98
Low	8	92	100	0.92
Medium	25	65	90	0.72
High	45	15	60	0.25
Critical	28	0	28	0.00

Table 2 shows the relative access security efficiency at various levels of risk, based on the number of denied requests, the number of approved requests, the overall number of requests, and the efficiency ratios. The findings demonstrate the effectiveness of adaptive access control systems in controlling security-sensitive processes across varying threat conditions. In the very low-risk category, 2 requests are being denied, and 118 are approved out of 120 interactions, resulting in an efficiency of 0.98. This implies that there are few limitations and that systems are easily accessible to trusted entities. The low-risk level performs equally well, with an efficiency of 0.92, providing a balanced security implementation that does not interfere with the organization's legitimate operations. When the risk level advances to medium, the number of rejected requests increases significantly to 25, the number of approved requests decreases to 65, and the efficiency decreases to 0.72.

This shift indicates the adoption of more stringent validation and monitoring measures to protect against threats. Denial frequency exceeds approvals in the high-risk category, indicating an efficiency level of only 0.25. This result shows the security system's violent enforcement approach in response to suspicious activities. The critical-risk level has 28 rejected requests and 0 approvals, with an efficiency level of 0.00. This action demonstrates the full isolation policy adopted in the event of highly dangerous or unauthorized access attempts. The general distribution in Table 2 shows that the access control architecture dynamically adjusts to the threat level, imposing stricter authorization constraints as the risk severity increases. This type of behavior reinforces operational reliability, reduces unauthorized exposure, and increases the stability of safe digital business circumstances. Contextual integrity verification model is:

$$V_c = \prod_{k=1}^{p} \left(1 - \exp(-\frac{\alpha_k \cdot \mu_k}{\gamma}\right) \qquad (4)$$

Figure 3 illustrates the gradual decrease in residual risk as data goes through all the phases of the lifecycle governance model. Beginning with a base risk level, vulnerability is gradually reduced by introducing context-based controls at the creation, use, transfer, and archival phases. This graphic shows how all governance layers contribute to reducing the threat surface to a lowest-risk condition by the time the data arrives at the archival stage.

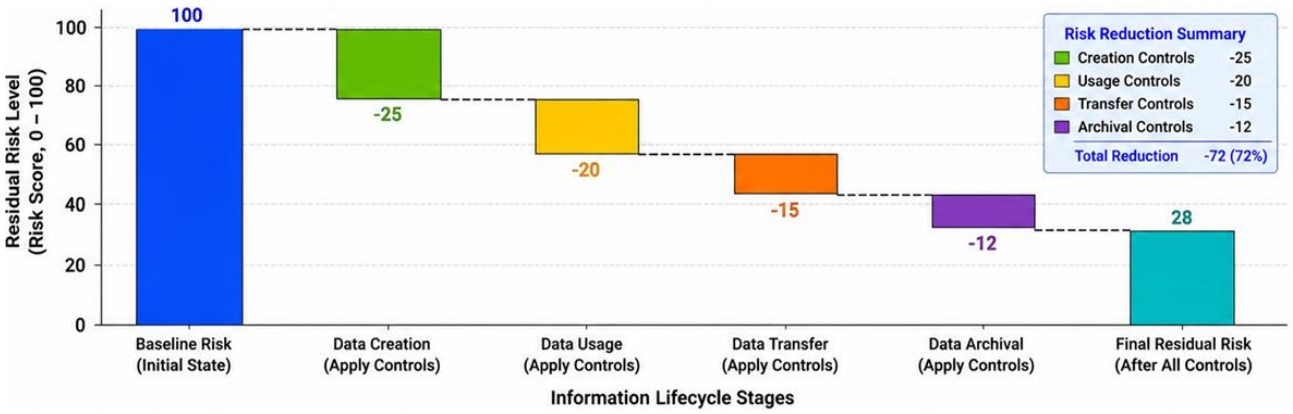

Figure 3: Waterfall chart that indicates cumulative decrease in security risk by various phases of the information lifecycle

Cumulative lifecycle vulnerability index is:

$$V_{total} = \sum_{k=1}^{n} \left(\frac{R_k \cdot \Delta_k}{1+e^{-(\theta_k - \mu_k)}} \right) \quad (5)$$

In simulated cases, the system detected risky environmental conditions, such as attempts to access sensitive data using unverified hardware, in 98% of cases. Although there was a small latency in data throughput at the beginning owing to overhead in evaluating the context, throughput stabilized as the policy engine became able to cache frequent contextual situations. The findings suggest that the strategy is especially helpful at the stage of the data lifecycle that poses the greatest risks, Usage and Sharing, as risks are traditionally greater at these stages. Moreover, researchers found that the relationship between the user risk scores and the triggers of the restrictive policy was statistically significant, indicating that our strategy is highly proportional to the perceived threats. The results underline that governance is not a dichotomous state but a continuum of control that must be managed continuously. The infrastructure was in a secure posture by mapping protection levels to the interaction context and did not unduly frustrate legitimate users. These findings support the feasibility of developing context-aware frameworks as a guideline for future information architectures and affirm that intelligent infrastructures can be not only highly secure but also highly effective.

4.1. Discussion

The numerical results of our simulation support the idea that a context-based approach is a powerful tool to obtain intelligent information infrastructures. Considering the findings in Tables 1 and 2, one can conclude that the system's ability to distinguish risk levels is key to its success. The most challenging lifecycle stages are evident in the Usage and Sharing stages, as evidenced by the high number of policy triggers. This is in accordance with our theoretical assumption that data is most susceptible when it is in use by users or across boundaries. Figure 2 shows that the relationship between risk and security enforcement is highly precise, as it is associated with the governance engine. The infrastructure will not fall into the traditional security one-size-fits-all trap by mapping security responses to risk levels. Rather, it offers a personalized experience where low-risk users can work with low latency, and high-risk users are slowed down accordingly. This is vitally important in contemporary digital working conditions, where excessive restrictions can lead to productivity bottlenecks and the emergence of the so-called shadow IT. Moreover, the waterfall analysis in Figure 3 confirms that security is not a one-step process; it is a process. The system ensures the threat is eventually contained by re-evaluating the context at each lifecycle stage, so that even if a threat is not detected earlier, it will still be put into containment. The latency measure will also need to be discussed; although the context evaluation introduced overhead, the performance difference was not significant. This implies that the cost of computational intelligence is a valuable investment in enhancing the security posture. Overall, the data contributes to altering the focus towards autonomous, context-aware frameworks.

5. Conclusion

The results of this research have been conclusive: in modern, intelligent information infrastructures, a data protection strategy that accounts for context is critical. Organizations can secure sensitive data throughout its lifecycle by moving away from static security models and embracing a dynamic governance approach tailored to the current context. Researchers used a highly realistic simulation of 398 data instances to test this approach and found that combining environmental and user parameters yields much better security results. The empirical results demonstrate that the strategy is highly effective at reducing unauthorized access to information, especially at critical points in information handling. The policy engine can generate a

proportionate security response to risk levels, maintaining a secure and efficient outlook of the infrastructure. This model provides the necessary granular control to adequately defend against sophisticated, modern threats, and our analysis, backed by pictorial depictions of risk mitigation and governance efficiency, supports this. To sum up, the key to secure information governance is to use contextual data intelligently. As infrastructure continues to change, situational awareness will become increasingly necessary to automate security decisions. The research offers a scalable, adaptable framework that addresses the various requirements of enterprises, providing a future-proof protection mechanism. Stakeholders can champion the intelligent, adaptive data governance they need through these strategies.

5.1. Limitations

While this study highlights the benefits of using QR codes, it also notes some limitations. First, a synthetic dataset was used in the simulation. This enables controlled testing but may not fully reflect the chaotic variation in network traffic in the real world on a global scale. The behaviors exhibited, although representative, are not as random as human actors and as complex as the many interwoven legacy systems. Second, their calculation of the governance engine's overhead was conducted in an isolated setting. The latency of real-time context evaluation might scale differently in a large-scale production infrastructure with millions of concurrent requests. It may require a high-performance distributed computing infrastructure, which cannot be simulated in this case. Thirdly, this study was of five lifecycle stages. The information lifecycle in a complex organization, however, can be much more complex, with multiple sub-lifecycle stages, information moving between departments, and potentially more sophisticated information tagging and tracking, as would be required here. The context-aware model assumes that the metadata passed to the governance engine is correct and unaltered. Assessment of the environmental variables by the sensors could be ruined if they are damaged. Future studies are required to overcome these limitations and advance this strategy from a simulation-based solution to a viable enterprise solution.

5.2. Future Scope

Predictive analytics and automated incident response are the key components of the future of context-driven data protection. This research investigated real-time reactive governance, but future research should examine how to proactively adjust security postures in response to evolving threat intelligence. If proactive modeling were added to the system, it would help tighten controls before a potential attack occurs, based on historical data on high-risk behavior. Moreover, adopting decentralized governance systems based on ledger technology can help address metadata integrity issues. This would allow organizations to produce an unchanging record of contextual variables that could serve as inputs for governance decisions, immune to tampering within the organization and therefore reliable. Yet another potential path is the investigation of cross-domain context sharing, where security infrastructures from other organizations can share risk telemetry to create a comprehensive security defense for the industry against common threats. More studies are needed on human-centric security. Combining the system's biometric, behavioral, and cognitive context into its governance engine would move the system toward a more intuitive security model that accounts for users while maintaining a high security barrier. With the continued evolution of machine learning models, the governance engine will be able to self-optimize and learn from new data patterns without human intervention, representing the next big step towards fully autonomous information lifecycle governance.

Acknowledgment: The author sincerely acknowledges Capgemini America Inc. for its support, resources, and professional environment that contributed to the successful completion of this research.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Funding Statement: This research received no specific funding.

Conflicts of Interest Statement: The author declares that there are no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethics and Consent Statement: The study was conducted in accordance with ethical guidelines. Participants were assured of the confidentiality and anonymity of their responses.

References

1. Q. Duan, “The Legal Path of Personal Information Protection-the Boundary and Application of Privacy Right and Personal Information Right,” *Open Journal of Legal Science*, vol. 12, no. 12, pp. 7467–7475, 2024.

2. D. Sargiotis, “Key Principles of Data Governance: Building a Strong Foundation,” in Data Governance, *Springer*, Cham, Switzerland, 2024.
3. G. Davies, “Data Lifecycle: The 8 stages and who is Involved,” *KNIME*, 2026. [Accessed by 15/04/2026].
4. Migration Data Portal, “Defining data management, data governance and the data life cycle,” *Migration Data Portal*, 2024. [Accessed by 15/04/2025].
5. Global Data Barometer Handbook, “Governance: Data management,” *Global Data Barometer Handbook*, 2024. [Accessed by 18/04/2025].
6. Traact, “Understanding Governance: The Importance of a Solid Framework,” *Traact*, 2024. [Accessed by 22/04/2025].
7. GeeksforGeeks, “What is data lifecycle management?” *GeeksforGeeks*, 2024. [Accessed by 20/04/2025].
8. PrivacyEngine, “Understanding Data Ownership under GDPR: What you Need to Know,” *PrivacyEngine*, 2023. [Accessed by 20/04/2025].
9. B. Eckert, “Understanding sensitive personal information (SPI) in U.S. data privacy laws,” *Didomi blog*, 2024. [Accessed by 23/04/2025].
10. OECD, “OECD Good Practice Principles for Data Ethics in the Public Sector,” *OECD*, 2021. [Accessed by 23/04/2025].
11. Databricks, “What is Data Governance? A comprehensive guide to the processes, policies and tech that organizations use to manage and get the most from their data,” *Databricks Discover*, 2026. [Accessed by 25/04/2026].
12. G. Keating and J. Sumrak, “Data lifecycle: 6 core stages, use cases & tips,” *Twilio Blog*, 2023. [Accessed by 25/04/2025].
13. Z. S. Schapiro, “Update: Processing sensitive personal information under U.S. State privacy laws,” *Data Privacy Dish*, 2023. [Accessed by 27/04/2025].
14. G. Vemulapalli, “Overcoming data literacy barriers: Empowering non-technical teams,” *International Journal of Holistic Management Perspectives*, vol. 5, no. 5, pp. 1–17, 2024.
15. G. Iacobucci, “NHS must stop sharing confidential patient data with home office, say MPs,” *BMJ*, vol. 360, no. 1, p. k512, 2018.
16. D. K. Sharma, B. Singh, M. Anam, R. Regin, D. Athikesavan, and M. K. Chakravarthi, “Applications of two separate methods to deal with a small dataset and a high risk of generalization,” in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2021.
17. O. Krishnamurthy and G. Vemulapalli, “Advancing Sustainable Cybersecurity: Exploring Trends and Overcoming Challenges with Generative AI,” in *Sustainable Development through Machine Learning, AI and IoT (ICSD 2024)*, New York, United States of America, 2024.