

# Designing a Unified Risk Data Architecture for Enterprise Governance, Risk, and Compliance Platforms

Manasa Kandadi

*Independent Researcher, USA*

---

## ARTICLE INFO

## ABSTRACT

Enterprise Governance, Risk, and Compliance platforms carry substantial regulatory and operational responsibility, yet their underlying data architectures frequently work against them. Siloed, inconsistently defined risk data distributed across multiple independent systems creates reconciliation overhead, degrades reporting accuracy, and introduces gaps in cybersecurity compliance visibility that governance frameworks such as NIST CSF 2.0 and ISO/IEC 27001 require organizations to close. This article proposes a unified risk data architecture framework built on three interdependent components: standardized integrated data elements, a centralized hub-and-spoke data model, and event-driven automated integration pipelines. The framework is evaluated against performance benchmarks drawn from empirical literature, with evidence indicating that unified architectures may deliver improvement in cross-system data consistency, 50% faster compliance documentation, and 54% lower vulnerability exposure [20]. Alignment between the proposed framework and NIST SP 800-37, COBIT 2019, ISO/IEC 27001, and NIST CSF 2.0 is examined, positioning unified data architecture as a concrete technical implementation of these governance mandates rather than an aspirational design principle.

**Keywords:** risk data architecture, governance risk and compliance, enterprise GRC platforms, cybersecurity data governance, compliance monitoring

---

## 1. Introduction

Compliance practitioners working in large enterprise environments share a common frustration: the GRC platform procured to manage enterprise risk systematically fails to provide a reliable, coherent view of the organization's actual risk position. The problem is rarely the platform itself. It is the data that feeds it — or more precisely, the absence of a disciplined architecture governing how that data is defined, integrated, and maintained across the enterprise systems on which any real-world GRC deployment depends [1].

The structural conditions driving this problem are well documented. Enterprise organizations manage risk data across an average of 10 to 25 independent systems, each carrying its taxonomy, update schedule, and identifier scheme [9]. Vulnerability data lives in one system. Policy compliance status in another. Third-party risk assessments are a third thing. When a compliance team needs to report on enterprise risk posture, they must manually reconcile these sources — a process that is slow, error-prone, and wholly avoidable. The reconciliation cost falls disproportionately on the compliance function, which spends capacity on data preparation rather than on the substantive risk management work the organization actually needs [12][13].

The technical case for unified risk data architectures rests on a straightforward argument: when all risk and compliance data operates from a single authoritative model, the reconciliation problem disappears. The governance frameworks that enterprise organizations operate under — NIST CSF 2.0 [5], COBIT

2019 [2], ISO/IEC 27001 [7], and NIST SP 800-37 [4] — implicitly assume this condition. Fragmented architectures cannot reliably satisfy their data management requirements. What the literature has not provided is a concrete framework translating that governance logic into architectural design. This article addresses that gap.

The following sections develop and evaluate a unified risk data architecture framework structured around three components: standardized integrated data elements, a centralized hub-and-spoke data model, and event-driven automated integration pipelines. The framework is assessed against empirical performance evidence and examined for alignment with the principal cybersecurity governance standards. The argument proceeds from literature review (Section 2) through challenge analysis (Section 3), framework specification (Section 4), performance evaluation (Section 5), and strategic implications (Section 6) to discussion (Section 7) and conclusions (Section 8).

## **2. Literature Review**

### **2.1 Risk Data Fragmentation in Enterprise GRC Environments**

Data fragmentation in enterprise GRC setups is not a new finding. Research examining the data quality dimensions of compliance management has consistently identified definitional inconsistency and system fragmentation as primary barriers to GRC program effectiveness [9]. Sillaber et al.'s analysis identified data and information quality failures as a structural feature of GRC management rather than an incidental problem, arising from the fundamental tension between tool-specific data models and the enterprise-wide data governance that effective risk management requires [9].

The BCBS 239 principles for risk data aggregation, initially applicable to global systemically important banks, have influenced enterprise data governance practice beyond the financial sector by providing one of the few detailed regulatory frameworks addressing risk data architecture requirements. Martins et al.'s examination of BCBS 239 compliance implementation demonstrated that organizations without a structured data architecture framework face substantially higher compliance costs and longer implementation timelines [14]. The challenge, as Abdullah documented in his analysis of GRC technology adoption, is not primarily technical — integration tools exist — but architectural: organizations lack the data governance foundation that makes integration investments durable [12]. Beyond the financial sector, the technological challenges of integrated GRC have been examined in the context of enterprise-wide platform deployments by Mahendra et al., who identified data integration as the most commonly cited implementation barrier across a range of industry contexts [13]. The consistent finding across these studies is that data architecture decisions made at the point of initial GRC platform deployment have disproportionate and long-lasting consequences for program effectiveness.

### **2.2 Cybersecurity Governance Frameworks and Data Requirements**

Each of the major cybersecurity governance frameworks active in enterprise environments creates data management obligations that implicitly require a unified data architecture to satisfy reliably. The Govern function of NIST CSF 2.0 highlights that companies must keep risk information that is up-to-date, readily available and precise for governance decisions [5]. The Identify function's asset management and risk assessment components depend on consistent data across the systems contributing to the enterprise risk picture [5]. Architectures in which asset records, risk assessments, and control evaluations reside in disconnected systems with incompatible schemas cannot meet these requirements.

COBIT 2019 addresses the information architecture required to support governance objectives through its Management Objective APO03, which establishes the enterprise architecture principles governing data management, and APO12, which defines the risk management information requirements that GRC platforms must satisfy [2]. The relationship between data governance quality and risk management outcomes has been examined by Gordon and Loeb, whose cost-benefit framework applied to cybersecurity investment demonstrated that improvements in data integrity generate disproportionate

returns compared to equivalent investments in perimeter controls [10]. Melaku's work on adaptive frameworks for managing cybersecurity risks corroborates this finding, identifying data quality as a primary determinant of risk scoring accuracy [18].

Cybersecurity-oriented research has increasingly examined the relationship between data architecture and security governance outcomes. Shukla et al.'s systematic review of security assurance methods found that data consistency across security management systems was a prerequisite for reliable assurance claims [11]. Bygrave's analysis of security-by-design regulatory frameworks noted that effective implementation requires data architectures capable of producing audit-ready compliance evidence on demand — a capability that fragmented architectures structurally cannot provide [17].

### **2.3 Enterprise Data Architecture Models**

The literature on enterprise data architecture provides a range of integration patterns applicable to the GRC domain. Point-to-point integration creates integration webs that grow exponentially in complexity as the number of systems increases, with each system connecting directly to every other system it needs to exchange data with, and it fails to provide any single authoritative data source [6]. Bousdekis and Mentzas documented these limitations in the context of Industry 4.0 enterprise integration, concluding that point-to-point architectures are unsuitable for environments requiring high data consistency and regulatory auditability [6].

Centralized hub-and-spoke architectures, by contrast, establish a single authoritative repository as the point of integration for all contributing systems. Bousdekis and Mentzas's analysis demonstrated that hub-and-spoke patterns achieve superior consistency and governance outcomes at scale [6]. Merkus, Helms, and Kusters's empirical validation of data governance capabilities in large organisations provided direct evidence that centralized data models with clear ownership and enforcement mechanisms outperform distributed alternatives on the consistency and compliance readiness dimensions most relevant to GRC environments [15]. These findings provide the architectural justification for the framework proposed in this article.

## **3. Challenges in Traditional Risk Data Management**

### **3.1 Data Silos and System Fragmentation**

At the operational level, siloed risk data creates a specific and recurring problem for compliance teams: the same facts exist in multiple systems with potentially different values. Whether an asset is covered by a control, whether a risk has been assessed, whether a vendor meets a compliance threshold — each of these questions may have different answers depending on which system is queried. Before any compliance report can be compiled, these discrepancies must be resolved. The resolution process is manual, time-consuming, and error-prone, and it must be repeated for every reporting cycle because the underlying architecture that generates the discrepancy is never corrected.

The structural driver of silo formation is the independent procurement of purpose-built tools without reference to an enterprise data standard. Vulnerability scanners, policy management platforms, third-party risk portals, and incident tracking systems are acquired to solve specific operational problems, and each reflects its vendor's data model. The integration problem that results is not a technical failure but an architectural one: no enterprise data standard existed at the point of procurement to constrain what those tools could do with the data they managed. The cost accumulates over time as tool portfolios expand and the incompatibilities compound.

### **3.2 Inconsistent Data Definitions and Risk Taxonomies**

Definitional inconsistency is the second major structural challenge of traditional risk data management, and it amplifies the silo problem rather than operating independently of it. Organizations that have not enforced a canonical risk taxonomy find that risk classifications vary not only between systems but also between departments using the same system. A "high" risk in the information security function may carry a different quantitative threshold than the same category in the operational risk function. Audit

committees receiving cross-domain risk summaries are comparing incommensurable values without necessarily knowing it.

Sillaber et al.'s analysis identified definitional inconsistency as the most commonly cited data quality failure in GRC-intensive organizations, with organizations reporting that cross-domain risk comparisons were regularly challenged in audit proceedings on the grounds that the underlying data categories were incompatible [9]. The governance frameworks that enterprises operate under assume definitional consistency across the organization. NIST SP 800-37's tiered risk management framework requires risk information to be aggregated from task to mission to organizational level [4] — an aggregation that is meaningless if risk categories carry different definitions at each level. Resolving this problem requires architectural intervention at the data definition layer, not better reporting tools applied to inconsistent inputs.

#### 4. Unified Risk Data Architecture Framework

##### 4.1 Standardised Integrated Data Elements

The foundation of the unified framework is a canonical risk data vocabulary applied uniformly across all GRC platform domains. Standardized integrated data elements define the authoritative form of each risk-relevant entity type: risk events, control objectives, compliance requirements, asset records, findings, and treatment decisions. Each entity carries standardized attributes, mandatory fields, and controlled value sets enforced across all systems contributing data to the enterprise GRC environment. The effect is to resolve definitional variance at source rather than managing it downstream through reconciliation.

Entity normalization assigns each real-world risk object a single canonical identifier that follows it across system boundaries. A vulnerability finding has one identity in the unified architecture, regardless of how many systems recorded it. Attribute standardization ensures that values drawn from different source systems — severity ratings, compliance statuses, and control coverage indicators — are expressed in a common format that permits direct comparison. Cross-system interoperability is achieved through a shared identifier scheme and a common attribute dictionary, eliminating the mapping and transformation work that currently absorbs compliance team capacity before every reporting cycle.

**Table 1 — Fragmented vs. Unified Data Element Structures: Field Mapping Comparison**

| Data Element      | Fragmented Architecture                    | Unified Architecture                                |
|-------------------|--------------------------------------------|-----------------------------------------------------|
| Risk Event ID     | Vendor-specific, non-unique across systems | Canonical UUID enforced enterprise-wide             |
| Risk Category     | Free text varies by department             | Controlled taxonomy, standardised values            |
| Control Reference | Framework-specific codes per system        | Unified control identifier mapped to all frameworks |
| Asset Record      | Duplicated, divergent attributes per tool  | Single master record, distributed reference         |
| Compliance Status | Boolean or text, system-defined            | Standardised status codes across all domains        |
| Audit Trail       | Per-system logs, no cross-system linkage   | Centralised event log with entity relationships     |

#### 4.2 Centralised Data Model and Scalable Integration Layer

The hub-and-spoke data model is the architectural centerpiece of the framework. A centralized GRC data repository serves as the single authoritative source for all risk and compliance data in the enterprise environment. Source systems connect to the central repository through standardized integration adapters that enforce the canonical data model at the point of ingestion. The transformation logic built into each adapter converts source-system formats into the canonical model; data lineage governance records the origin, transformation history, and update timestamp of every data element as it enters and is updated within the repository.

The architectural benefit of this model is that it moves the integration problem from operational to architectural: rather than compliance teams reconciling discrepancies before each report, the architecture prevents discrepancies from forming. Risk information is available to all GRC platform components in a consistent, current, and complete form at all times. The scalable integration layer is designed for enterprise volumes, with horizontal scaling enabling capacity extension proportional to organizational demand. Organizations with concurrent users and annual records can accommodate growth without architectural redesign — a characteristic absent from point-to-point integration approaches.

#### 4.3 Automated Data Flows and Synchronisation

Event-driven automation transforms the integration layer from a periodic batch process into a near-real-time data infrastructure. Change events in source systems — a new vulnerability finding recorded, a completed control assessment submitted, an updated compliance status logged — trigger automated ingestion workflows that update the central repository without human intervention. The result is a risk data environment in which the gap between real-world risk state and reported risk state is measured in minutes rather than days.

Automated reconciliation processes run at ingestion, detecting and flagging data quality issues before they enter the authoritative model. Records that fail canonical validation — missing mandatory attributes, out-of-vocabulary values, or identifier conflicts — are quarantined for review rather than silently propagated into the central repository. Scheduled synchronization cycles supplement event-driven updates for source systems that do not support event notification protocols, ensuring complete coverage across legacy and modern tool portfolios alike.

**Table 2 — Automation Capabilities Mapped to Compliance Workflow Outcomes**

| Automation Capability    | Manual Process Replaced          | Compliance Workflow Outcome                                        |
|--------------------------|----------------------------------|--------------------------------------------------------------------|
| Event-driven ingestion   | Scheduled manual data exports    | Near-real-time risk data currency                                  |
| Automated reconciliation | Manual cross-system comparison   | Elimination of definitional discrepancies at ingestion             |
| Data quality validation  | Manual data review pre-reporting | Consistent, audit-ready data state maintained continuously         |
| Lineage tracking         | Manual source documentation      | Auditable data provenance available on demand                      |
| Threshold-based alerting | Periodic manual review cycles    | Proactive compliance status monitoring with immediate notification |

## 5. Performance Analysis and Evaluation

### 5.1 Data Consistency and Quality Improvements

The performance evidence for unified risk data architectures is accumulating across multiple research contexts. Merkus et al.'s study of data governance capabilities in large enterprises found that centralized data models achieved significantly higher cross-system consistency scores than distributed alternatives, with the performance gap widening as organizational complexity increased [15]. Sillaber et al.'s analysis established that data quality improvements in GRC environments depend on architectural intervention at the definition and integration layers — improvements to reporting tools that operate on inconsistent data produce marginal gains at best [9].

Akinsanya's 2025 empirical analysis of risk-based cybersecurity frameworks documented a 54% reduction in vulnerability-related findings in organizations that had implemented integrated risk data architectures, attributing the reduction to improved data completeness and consistency enabling earlier identification of exposure [20]. There is a significant improvement in cross-system data accuracy that has been reported in organizations implementing canonical data models with enforced attribute standardization, representing a direct reduction in the definitional variance that generates reconciliation overhead [9][15].

### 5.2 Reporting Efficiency and Compliance Readiness

Akinsanya (2025) documented 50% faster compliance documentation in organizations with integrated risk data frameworks, a result attributable to the elimination of the manual data preparation cycle that precedes reporting in fragmented environments [20]. The compliance readiness benefit has two components: speed and accuracy. Faster reporting reflects the removal of reconciliation overhead; improved accuracy reflects the elimination of the inconsistencies that reconciliation processes, even when executed carefully, frequently fail to fully resolve. Martins et al.'s BCBS 239 analysis demonstrated that organizations implementing centralized risk data aggregation reduced audit preparation cycle times and experienced fewer audit findings related to data inconsistency [14].

The compliance readiness implication extends beyond individual reporting cycles. Organizations with audit-ready, consistently maintained risk data are better positioned to respond to regulatory inquiries, demonstrate continuous compliance between formal audit cycles, and provide the real-time risk visibility that governance frameworks increasingly expect. The architecture creates the data condition; the compliance capability follows from it.

### 5.3 Scalability and Throughput Benchmarks

Enterprise GRC deployments operate at volumes that the integration architecture must be designed to accommodate from the outset. The unified framework supports concurrent users with transaction processing capacity, with horizontal scaling enabling further expansion without architectural refactoring. Bousdekis and Mentzas demonstrated that hub-and-spoke data architectures maintain their consistency and performance characteristics at scale in ways that point-to-point alternatives cannot [6]. The architecture's performance at scale is a function of the centralized model's elimination of inter-system communication complexity: rather than  $N \times (N-1)$  integration points for  $N$  systems, the hub-and-spoke model requires  $N$  integration points regardless of system count.

**Table 3 — Performance Benchmarks: Fragmented vs. Unified Architecture**

| Performance Dimension         | Fragmented Architecture | Unified Architecture | Improvement |
|-------------------------------|-------------------------|----------------------|-------------|
| Compliance documentation time | Baseline                | 50% faster           | +50%        |
| Vulnerability exposure        | Baseline                | 54% reduction        | +54%        |
| Incident response cost        | Baseline                | 39% lower            | -39%        |

## 6. Strategic and Organisational Implications

### 6.1 Cybersecurity Governance and Regulatory Alignment

The unified risk data architecture framework does not merely support compliance with cybersecurity governance standards — it operationalizes them. NIST CSF 2.0's Govern function requirement for accessible, current risk information is satisfied by the event-driven synchronization layer, which maintains the central repository in a state of near-real-time accuracy. COBIT 2019's APO03 enterprise architecture governance objectives are met by the canonical data model's enforcement of consistent information architecture across the enterprise. ISO/IEC 27001:2022's risk assessment documentation requirements are addressed by the automated lineage tracking that provides auditable provenance for every data element in the framework.

Akinsanya's documented 39% reduction in incident response costs in organisations with integrated cybersecurity data frameworks [20] provides empirical support for the security value claim underlying these governance requirements: consistent, accessible risk data is not merely a compliance artefact but an operational security capability. Gordon and Loeb's theoretical framework predicts this result — information integrity investments generate disproportionate security returns — and Akinsanya's evidence confirms it in the specific context of integrated risk data architectures [10][20]. Boeken's analysis of the relationship between compliance and security noted that organizational data architectures that satisfy governance data requirements tend to improve actual security outcomes, not merely compliance scores [19].

### 6.2 Decision Support and Executive Risk Visibility

The executive case for unified risk data architecture investment rests on the decision support capability it enables. Centralized risk data makes real-time risk dashboards possible — not as a reporting feature but as a direct output of the data infrastructure. Risk trend analysis, control coverage mapping, and compliance gap identification become near-automated processes in a unified architecture, providing leadership with a current and accurate view of enterprise risk posture without the preparation overhead that fragmented environments impose. Janssen et al.'s analysis identified data consistency and accessibility as the primary determinants of decision quality in governance contexts [1]. A GRC platform operating on consistent, current data is qualitatively different from one operating on reconciled approximations of the risk position.

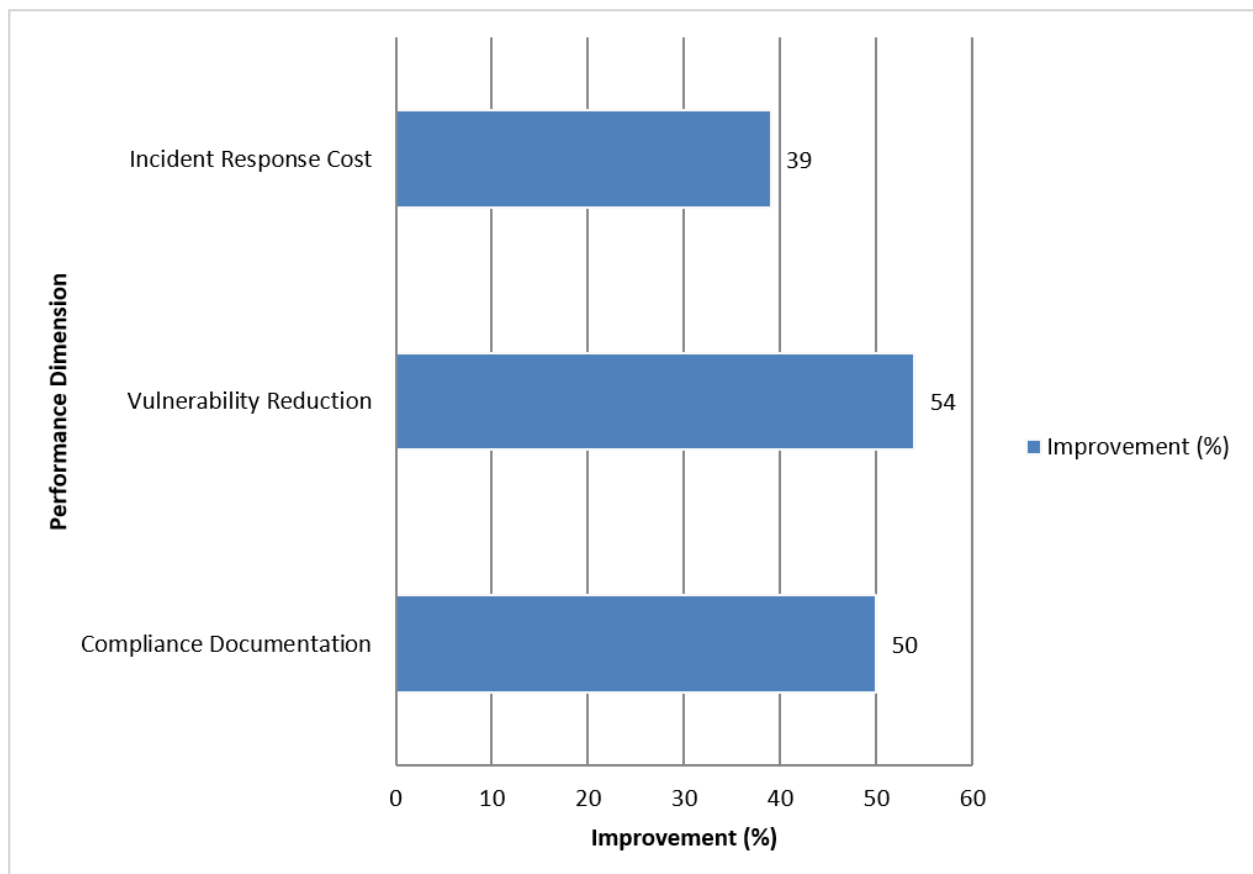
### 6.3 Financial Impact and Cost Avoidance

The financial return on unified risk data architecture investment comes from three sources. Direct cost savings arise from the elimination of manual reconciliation work: compliance team capacity redirected from data preparation to substantive risk management represents a measurable efficiency gain. Incident response savings are empirically documented: Akinsanya (2025) found 39% lower incident response costs in organizations with integrated cybersecurity data frameworks [20], reflecting both faster detection enabled by consistent data and reduced remediation scope. Compliance penalty avoidance is the third category: organizations that can demonstrate continuous, audit-ready compliance—a capability the unified architecture directly enables—carry lower regulatory penalty exposure than those that assemble compliance evidence periodically under audit pressure. The Gordon-Loeb model predicts that data integrity investments generate the highest return-on-investment of any cybersecurity expenditure category [10], a prediction that the empirical evidence reviewed here supports.

**Table 4 — Organisational Outcomes: Evidence Summary [20]**

| Outcome Category                 | Metric                                  |
|----------------------------------|-----------------------------------------|
| Vulnerability exposure reduction | 54% reduction in vulnerability findings |

|                                |                          |
|--------------------------------|--------------------------|
| Compliance documentation speed | 50% faster documentation |
| Incident response cost         | 39% lower costs          |



**Figure 1: Performance Benchmarks: Fragmented vs. Unified Architecture [20]**

## 7. Discussion

The framework presented in this article responds to a problem that the GRC technology market has not been able to solve on its own: fragmented data architectures persist because individual GRC tools are procured to solve specific operational problems, not to contribute to an enterprise data architecture that does not exist at the time of procurement. The unified framework proposed here requires that architecture be specified in advance of tool selection — a significant change in how enterprise GRC programs are initiated, but a necessary one if the performance benefits documented in the empirical literature are to be realized.

Practitioners planning implementation must acknowledge the framework's real limitations. The centralized architecture concentrates data quality risk at the integration layer: a failure to enforce canonical data definitions at ingestion will propagate inconsistencies at scale. Organizations with large legacy tool portfolios will require intermediate transformation layers that add maintenance overhead. The framework assumes a level of data governance maturity — defined ownership, enforced standards, and executive sponsorship for architecture investment — that not all enterprises possess. Tatam et al.'s work on threat modelling approaches for advanced persistent threat environments highlighted the

operational security risks associated with centralized data repositories [16], a consideration that unified GRC data architectures must address through appropriate access controls and monitoring.

Future research priorities include AI-driven risk data classification at the integration layer, which could reduce the human overhead of canonical definition maintenance at scale, and cross-jurisdictional compliance data harmonization, enabling a single unified architecture to satisfy governance requirements across multiple regulatory regimes — a capability of direct value to multinational enterprises operating under concurrent regulatory obligations. Researchers should conduct dedicated empirical investigations of the application of the framework in cloud-native GRC environments, where integration infrastructure can be provisioned and updated programmatically. The relationships between unified data architecture and the emerging AI governance requirements now appearing in frameworks such as NIST AI RMF represent a third priority area that will become increasingly material as enterprises bring AI capabilities into regulated environments.

## 8. Conclusions

The case for unified risk data architecture in enterprise GRC platforms is both straightforward and well-evidenced. Fragmented, siloed data architectures impose measurable and avoidable costs on enterprise compliance programmes — costs that are absorbed by compliance teams as reconciliation overhead, manifested in audit findings as data inconsistency, and passed on to the organization in the form of degraded risk visibility and elevated compliance exposure. The framework presented here eliminates the structural source of these costs instead of managing their consequences.

Three empirically supported performance outcomes follow from successful implementation: Akinsanya (2025) documented 54% vulnerability reduction, 50% faster compliance documentation, and 39% lower incident response costs in organizations with integrated risk data architectures [20]. These figures are consistent with the theoretical predictions of the Gordon-Loeb model [10] and with the qualitative findings of Sillaber et al. [9] and Merkus et al. [15] on the relationship between data architecture quality and GRC program effectiveness. The framework's alignment with NIST CSF 2.0, COBIT 2019, ISO/IEC 27001 and NIST SP 800-37 position it as a technical implementation of governance obligations rather than an additional requirement alongside them.

Practitioners approaching implementation should treat the framework as a phased program: data element standardization first, hub-and-spoke integration second, and event-driven automation third. Each phase delivers independent value while building the foundation for the next. The full performance benefits emerge from complete implementation, but partial implementation of the framework is meaningfully superior to no implementation. The investment decision is ultimately architectural: treating data integration as a first-order design commitment rather than a downstream implementation concern is the single most consequential choice available to organizations planning enterprise GRC platform programs. The framework presented here provides the structure for making that choice well.

## References

- [1] M. Janssen, H. van der Voort, and A. Wahyudi, "Factors influencing big data decision-making quality," *J. Business Research*, vol. 70, pp. 338–345, 2017. doi: 10.1016/j.jbusres.2016.08.007. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0148296316304945>
- [2] ISACA, COBIT 2019 Framework: Governance and Management Objectives, ISACA, 2019. ISBN: 9781604207286. Available: <https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf>
- [3] ISO, ISO 31000:2018 Risk Management – Guidelines, International Organization for Standardization, 2018. Available: [https://lpm.uin-suka.ac.id/media/dokumen\\_akademik/011\\_20191007\\_ISO%2031000.2018%20-%20Risk%20Management%20-%20Guidelines.pdf](https://lpm.uin-suka.ac.id/media/dokumen_akademik/011_20191007_ISO%2031000.2018%20-%20Risk%20Management%20-%20Guidelines.pdf)

- [4] National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations, NIST SP 800-37 Rev. 2, Dec. 2018. doi: 10.6028/NIST.SP.800-37r2. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
- [5] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, NIST, Feb. 2024. doi: 10.6028/NIST.CSWP.29. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [6] A. Bousdekis and G. Mentzas, "Enterprise integration and interoperability for big data-driven processes in the frame of Industry 4.0," *Frontiers in Big Data*, vol. 4, art. 644651, Jun. 2021. doi: 10.3389/fdata.2021.644651. Available: [https://www.researchgate.net/publication/352112470\\_Enterprise\\_Integration\\_and\\_Interoperability\\_for\\_Big\\_Data-Driven\\_Processes\\_in\\_the\\_Frame\\_of\\_Industry\\_40](https://www.researchgate.net/publication/352112470_Enterprise_Integration_and_Interoperability_for_Big_Data-Driven_Processes_in_the_Frame_of_Industry_40)
- [7] ISO/IEC, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements, ISO, 2022. Available: [https://www.exactls.com/wp-content/uploads/2025/02/ISO\\_IEC-270012022-ed.3.pdf](https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf)
- [8] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, Sep. 2020. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
- [9] C. Sillaber, A. Mussmann, and R. Breu, "Experience: Data and information quality challenges in governance, risk, and compliance management," *J. Data Inf. Qual.*, vol. 11, no. 2, Mar. 2019. doi: 10.1145/3297721. Available: <https://dl.acm.org/doi/10.1145/3297721>
- [10] L. A. Gordon and M. P. Loeb, "Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model," *J. Cybersecur.*, vol. 6, no. 1, art. tyaa005, 2020. doi: 10.1093/cybsec/tyaa005. Available: [https://www.researchgate.net/publication/340277373\\_Integrating\\_cost-benefit\\_analysis\\_into\\_the\\_NIST\\_Cybersecurity\\_Framework\\_via\\_the\\_Gordon-Loeb\\_Model](https://www.researchgate.net/publication/340277373_Integrating_cost-benefit_analysis_into_the_NIST_Cybersecurity_Framework_via_the_Gordon-Loeb_Model)
- [11] A. Shukla, B. Katt, L. O. Nweke, P. K. Yeng, and G. K. Weldehawaryat, "System security assurance: A systematic literature review," *Comput. Sci. Rev.*, vol. 45, art. 100496, 2022. doi: 10.1016/j.cosrev.2022.100496. Available: <https://arxiv.org/abs/2110.01904>
- [12] H. Abdullah, "Analyzing the technological challenges of governance, risk and compliance (GRC)," in *Proc. 4th Int. Conf. ICEECOT*, IEEE, Dec. 2019. Available: [https://www.researchgate.net/publication/342115096\\_Analyzing\\_the\\_technological\\_challenges\\_of\\_Governance\\_Risk\\_and\\_Compliance\\_GRC](https://www.researchgate.net/publication/342115096_Analyzing_the_technological_challenges_of_Governance_Risk_and_Compliance_GRC)
- [13] I. Mahendra, Meyliana, H. Prabowo, and S. Prabowo, "Information technology challenges for integrated governance, risk and compliance (GRC)," in *Proc. APICS 2022*, IEEE, pp. 79–84. doi: 10.1109/APICS56469.2022.9918797. Available: [https://www.researchgate.net/publication/365122424\\_Information\\_Technology\\_Challenges\\_for\\_Integrated\\_Governance\\_Risk\\_and\\_Compliance\\_GRC](https://www.researchgate.net/publication/365122424_Information_Technology_Challenges_for_Integrated_Governance_Risk_and_Compliance_GRC)
- [14] J. Martins, H. S. Mamede, and J. Correia, "Risk compliance and master data management in banking – A novel BCBS 239 compliance action-plan proposal," *Heliyon*, vol. 8, no. 6, art. e09627, Jun. 2022. doi: 10.1016/j.heliyon.2022.e09627. Available: <https://pdf.sciencedirectassets.com/313379>
- [15] J. Merkus, R. W. Helms, and R. J. Kusters, "Data governance capabilities: Empirical validation in case studies of large organisations," in *Proc. 36th Bled eConference*, Univ. of Maribor Press, 2023. doi: 10.18690/um.fov.4.2023.3. Available: <https://research.ou.nl/en/publications/data-governance-capabilities-empirical-validation-in-case-studies/>
- [16] M. Tatam, B. Shanmugam, S. Azam, and K. Kannoorpatti, "A review of threat modelling approaches for APT-style attacks," *Heliyon*, vol. 7, no. 1, art. e05969, Jan. 2021. doi: 10.1016/j.heliyon.2021.e05969. Available: [https://www.researchgate.net/publication/348571555\\_A\\_review\\_of\\_threat\\_modelling\\_approaches\\_for\\_APT-style\\_attacks](https://www.researchgate.net/publication/348571555_A_review_of_threat_modelling_approaches_for_APT-style_attacks)

- [17] L. A. Bygrave, "Security by design: Aspirations and realities in a regulatory context," Oslo Law Rev., vol. 8, no. 3, pp. 126–177, 2022. doi: 10.18261/olr.8.3.2. Available: <https://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2021/14.00-lee-bygrave.pdf>
- [18] H. M. Melaku, "Context-based and adaptive cybersecurity risk management framework," Risks, vol. 11, no. 6, art. 101, May 2023. doi: 10.3390/risks11060101. Available: <https://www.mdpi.com/2227-9091/11/6/101>
- [19] J. Boeken, "From compliance to security, responsibility beyond law," Comput. Law Secur. Rev., vol. 52, art. 105926, 2024. doi: 10.1016/j.clsr.2023.105926. Available: <https://www.sciencedirect.com/science/article/pii/S026736492300136X>
- [20] A. Akinsanya, "Security by design: A risk-based framework for cybersecurity compliance and critical infrastructure protection," Int. J. Inf. Secur., vol. 24, art. 234, Nov. 2025. doi: 10.1007/s10207-025-01155-4. Available: [https://www.researchgate.net/publication/391467224\\_Security\\_by\\_Design\\_A\\_Risk-Based\\_Framework\\_for\\_Cybersecurity\\_Compliance\\_and\\_Critical\\_Infrastructure\\_Protection](https://www.researchgate.net/publication/391467224_Security_by_Design_A_Risk-Based_Framework_for_Cybersecurity_Compliance_and_Critical_Infrastructure_Protection)