P-ISSN: 3050-9572 E-ISSN: 3050-9580

EUROPEAN DATA SCIENCE JOURNAL

Volume: 01 Issue: 01

RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

AI Risk Governance in Data Centers

Niklas Andersson

Asst Professor

Abstract

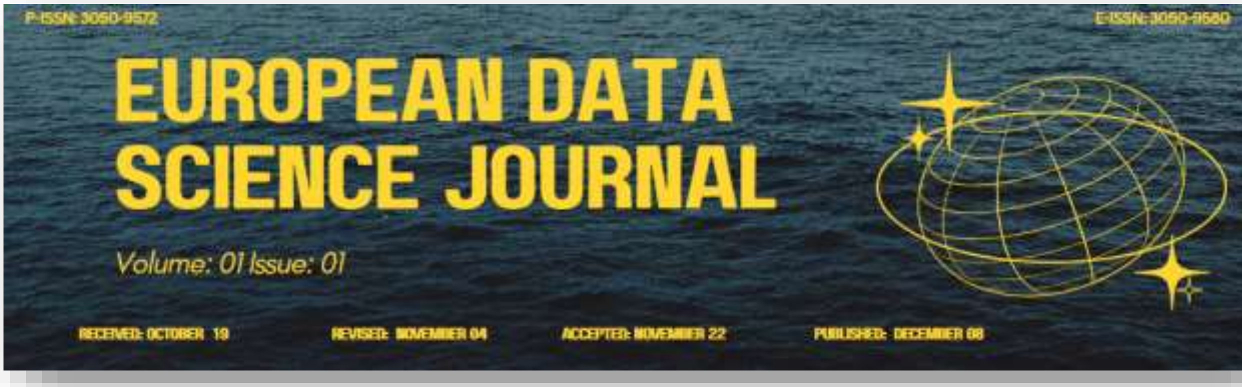
Governance, risk, and compliance form the foundation of responsible operations for any enterprise. The increasing business-aligned service delivery for data centers, accompanied by their growing adoption of AI-based technologies, such as predictive and anomaly detection analytics, necessitate further investigation into compliance and risk management frameworks in the context of intelligent data center operations. An AI-driven enterprise risk and compliance governance framework is proposed to support intelligent operations by establishing end-to-end AI service delivery and violation detection for externally imposed regulations and enterprise-defined standards. The risk management framework identifies key risk sources-classified as operational, cybersecurity, reliability, regulatory, and vendor-and proposes a scoring mechanism based on impact, likelihood, and detectability. The outcome of the risk-management framework aids development of a corresponding regulatory and compliance landscape covering data sovereignty, privacy, and protection; data quality, safety and security; industrial safety; and service and products. By capturing end-to-end AI service delivery requirements and integrating the necessary governance signal-processing technologies, the AI-driven enterprise risk and compliance governance framework provides a holistic perspective to support intelligent data center operations.

Keywords: Risk management, Compliance governance, Data centers, Anomaly detection, Predictive analytics .

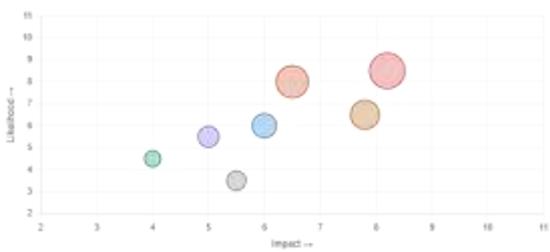
1. Introduction

The AI-driven enterprise risk and compliance governance framework presented here caters to the needs and concerns of regulators, business leaders, risk managers, and compliance officers for intelligent data center operations. Effective governance of technology operations is critical for business sustainability and legal compliance. A risk framework maps the enterprise risk landscape, for both AI technologies and data center operations, focusing on risk identification and classification. Regulatory instruments that lay the foundation for compliance governance form a compliance foundation. The implications of the data residency requirement of the Spanish Data Protection Regulation across all fifteen jurisdictions of the Data Protection & Privacy Policy Framework of the Organization of American States, supplemented by the provisions of the General Data Protection Regulation, illustrate the practical impact on operations. Authentic anomaly detection-based monitoring for risk management and predictive alerting for planning and optimization are proposed to address operational risk management and security risk management, respectively. AI technologies—primarily machine learning, augmented with deep learning and time series analysis—are the primary enablers of risk management.

It also includes any monitoring prescribed by external regulation or oversight for compliance or assurance purposes, together with the controls applied through the data center supply chain. The primary regulating forces can be external (for example, from governments and regulatory bodies) or internal (for example, from organization and management policies).



Flow Chart 1: AI-Driven Enterprise Governance Architecture

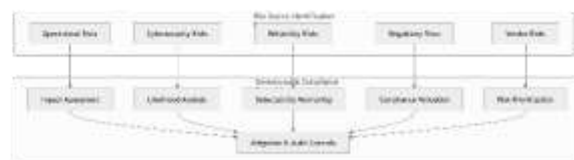


Graph 1 — Risk Scoring Matrix: Plots all 7 risk sources (operational, cybersecurity, reliability, regulatory, vendor, innovation, corporate governance) by impact vs. likelihood, with bubble size encoding detectability difficulty. Cybersecurity and operational risks cluster in the high-threat zone.

2. Foundations of AI-Driven Governance in Data Centers

2.1. Definitions and scope. AI-driven enterprise risk and compliance (GRC) governance encompasses both risk management and oversight for intelligent data center operations using the same resourcing principles. Following these principles can improve efficiency and effectiveness through data sharing, reuse, automating anomaly detection and risk prediction, and other recognized applications. AI governance refers specifically to GRC applied to the AI element of data center operations; AI-enabled enterprise GRC refers more broadly to leveraging AI in GRC.

An intelligent data center is a data center employing a modular, interoperable, scalable, and secure architecture for operational support based on a common operational decision model across the full operation lifecycle; these principles facilitate AI-enabled GRC governance. Risk surrounds potential events that threaten the achievement of enterprise objectives. Risk management involves identifying, assessing, controlling, and monitoring risk. Risk identification recognizes events that could confer a significant risk. Risk compliance governance incorporates evaluating the severity of the risks and monitoring their mitigation.



Flow Chart 2: Enterprise Risk Identification & Compliance Mapping

Risk Category	Primary Risk Source	Example Threats	Business Impact	Monitoring Method
Operational Risk	Internal Processes	Misconfiguration, Process Failure	Service Disruption	AI-Based Operational Analytics
Cybersecurity Risk	External/Internal Threats	Malware, Unauthorized Access	Data Breach	Anomaly Detection Systems
Reliability Risk	Infrastructure Failure	Downtime, SLA Violation	Revenue Loss	Predictive Maintenance
Regulatory Risk	Compliance Violations	GDPR Breach, Data Residency Failure	Legal Penalties	Compliance Monitoring Engines
Vendor Risk	Third-Party Dependencies	Supply Chain Failure	Operational Instability	Vendor Governance Analytics

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

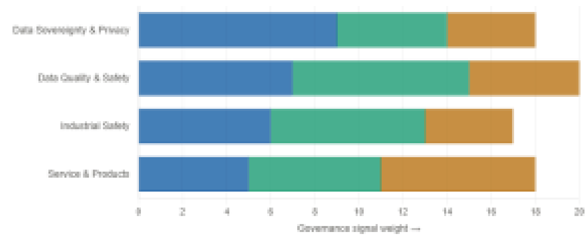
Risk Category	Primary Risk Source	Example Threats	Business Impact	Monitoring Method
Innovation Risk	Emerging Technologies	Unvalidated AI Deployment	Strategic Failure	AI Governance Validation
Corporate Governance Risk	Policy Weaknesses	Lack of Oversight	Reputation Damage	Governance Auditing

Table 1. Enterprise Risk Classification Matrix

2.1. Definitions and scope

Artificial Intelligence (AI) governance encompasses values, guardrails, and frameworks to enable (reliable, ethical, sustainable, fair) AI system development, deployment, and use. AI systems form end-to-end AI solutions together with smart infrastructure and AI-driven business processes. The AI governance framework must therefore also guide lower-level governance domains, such as Enterprise Risk and Compliance Governance in Intelligent Data Center Operations.

Intelligent Cloud and Edge Data Center Operations utilize AI-enabled solutions to enhance application, platform, and infrastructure services and their delivery. AI can also help to manage these solutions by detecting and predicting operational anomalies and failures, governance and regulatory compliance violations, and other forms of business and service risk. There exists considerable regulatory and standards requirements for AI, making AI Governance essential. The operational environment within which AI systems are built, managed, and operated introduces new AI Governance concerns. Risks arise from the operational environment, from external attackers and insider threats, from reliability and converged/indexed service availability, and from vendor dependencies.



Graph 2 — Compliance Governance Landscape: A stacked horizontal bar chart visualising the four compliance domains from the paper (data sovereignty & privacy, data quality & safety, industrial safety, service & products) broken down by signal type: external regulatory requirements, standards/frameworks, and internal policies. Data sovereignty carries the heaviest regulatory load.

3. Risk Management Framework for Intelligent Data Centers

Failure to identify existing and emergent risks in data center operations can cripple the enterprise by adversely affecting service delivery, damaging reputation, incurring financial penalties, and/or exposing the enterprise to regulatory scrutiny. Risk management is part of governance and compliance by ensuring that risk exposure is appropriately monitored and controlled. A risk management framework for risk identification and classification is presented that establishes a catalogue of significant existing and emergent risks in the context of intelligent data center operations.

Seven risk sources have been identified that, if realized, could damage reputation, incur financial penalties, and/or expose the enterprise to regulatory scrutiny: operational, cybersecurity, reliability, regulatory, vendor, innovation, and corporate governance. For each risk source, a list of candidate risks is provided that could affect operations in an intelligent data center. A classification scheme based on severity, likelihood, and detectability/monitorability helps quantify the risk of individual items, providing a basis for a prioritised risk management approach where effort is directed towards

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

addressing the most severe risks with the least processing overhead.

Failure to identify existing and emergent risks can cripple the enterprise by adversely affecting service delivery, damaging reputation, incurring financial penalties, and/or exposing the enterprise to regulatory scrutiny. Risk management is part of governance and compliance by ensuring that risk exposure is appropriately monitored and controlled. A risk management framework for risk identification and classification is presented that establishes a catalogue of significant existing and emergent risks in the context of intelligent data center operations.

Mathematical Formulas:

1. Risk Priority Number (RPN) for Governance Risk Assessment

$$RPN = I \times L \times D$$

Where:
I= Impact,
L= Likelihood,
D= Detectability.

Used for prioritizing operational, cybersecurity, regulatory, and vendor risks in intelligent data center environments.

2. Compliance Violation Score

$$CVS = \frac{N_v}{N_t}$$

Where:
N_v= Number of detected violations,
N_t= Total monitored compliance controls.

Represents overall governance compliance exposure.

3. Anomaly Detection Function

$$A(x) = | x - \mu | > \theta$$

Where:
x= Observed operational metric,
μ= Mean operational behavior,
θ= Detection threshold.

Used for identifying abnormal operational activities and failures.

4. Predictive Risk Forecasting Model

$$\hat{R}_{t+1} = f(R_t, X_t)$$

Where:
$\hat{R}_{t+1}$= Predicted future risk,
R_t= Current risk state,
X_t= Operational indicators.

Supports predictive analytics for intelligent governance.

5. Data Governance Trust Score

$$T_s = \frac{Q + S + P}{3}$$

Where:
Q= Data quality score,
S= Security score,
P= Privacy compliance score.

Measures trustworthiness of governance data pipelines.

6. SLA Reliability Equation

$$Rel = \frac{Uptime}{Total\ Time}$$

Used to evaluate service reliability and SLA adherence in intelligent data center operations.

7. Cybersecurity Threat Probability

$$P(T) = \frac{N_a}{N_s}$$

Where:
N_a= Number of successful attacks,
N_s= Total security events monitored.

Represents cyber-risk occurrence probability.

8. AI Governance Efficiency Metric

$$GE = \frac{A_d}{T_p}$$

Where:
A_d= Automated detections,
T_p= Total processed governance events.

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

Measures effectiveness of AI-assisted governance automation.

9. Data Lineage Integrity Equation

$$LI = \frac{D_t}{D_o}$$

Where:
D_t= Traceable data elements,
D_o= Original data elements.

Used for validating metadata lineage and provenance tracking.

10. Governance Alert Confidence Score

$$C_a = 1 - \frac{F_p}{T_a}$$

Where:
F_p= False positive alerts,
T_a= Total alerts generated.

Flow Chart 3: AI-Based Anomaly Detection & Predictive Analytics Pipeline

3.1. risk identification and classification

Data centers are vulnerable to multiple types of risk, including those related to operations, cybersecurity, service reliability, regulations, and vendors. Sources of operational risk include human actions (e.g., misconfigurations, data loss) as well as machine errors (e.g., hardware failure, application error, process fault). Cybersecurity risk is rising as operations rely on yet more external services, thus creating exposure to third-party breaches. Reliability risk stems from the possibility of service unavailability, latency, or other non-compliance with service level agreements (SLAs). Regulatory risk arises when operations breach regulations such as data residency, privacy, or protection laws. Third-party services expose data centers to the risk of non-compliance with these regulations. Vendor risk is the possibility of negative impact from the selection of suppliers. Unreliable or insecure vendors introduce operational risk, while untrustworthy suppliers can adversely affect service quality and availability.

Governance Component	**Objective**	**AI Technique Used**	**Compliance Focus**
Data Sovereignty Monitoring	Ensure regional data compliance	Rule-Based Analytics	GDPR & Residency Laws
Privacy Protection Engine	Protect PII data	Access Pattern Analysis	Privacy Governance
Auditability Framework	Maintain traceability	Log Correlation AI	Regulatory Audits
Encryption Governance	Secure data at rest/in transit	AI Policy Validation	Security Compliance
Consent Management	Track user permissions	NLP-Based Consent Parsing	User Data Rights
Cross-Border Data Control	Monitor external transfers	Predictive Risk Models	International Regulations

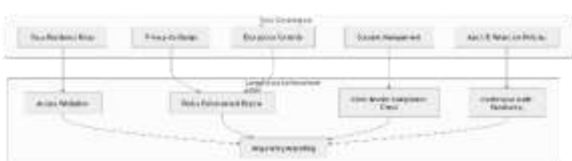
Table 2. AI-Driven Compliance Governance Components

4. Compliance Governance in Practice

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

Intelligent data centers are susceptible to a broad array of operational, compliance, cybersecurity, and reliability risks, the mitigation of which requires an auditable governance framework. Compliance governance defines the collection of regulations, standards, and frameworks (governance and compliance signals) that an organization must adhere to in its data center operations. Compliance signals reside primarily in external regulatory frameworks such as the General Data Protection Regulation (GDPR), applicable industry standards, and the organizations' internal policies and procedures. Gaps between compliance signals and current controls can also create additional risk that must be managed. Solutions that ease adherence to these signals and reduce the risk category fall under compliance governance.

Data sovereignty, privacy, and protection are the most significant compliance signals for operational management in current intelligent data centers. Organizations must satisfy jurisdictional requirements for data residency, adopt privacy-by-design principles, restrict access to sensitive data, ensure data is encrypted both at rest and in transit, and provide audit capabilities for access and management. In addition, organizations should obtain consent from data subjects (where required), specify data retention requirements, establish an audit and breach notification process, and adhere to local laws or appointed industry standards for data stored outside their jurisdiction.



Flow Chart 4: Data Sovereignty & Privacy Governance Framework

4.1. data sovereignty, privacy, and protection

The jurisdictional requirements for data residency, privacy, and protection play a significant role in the compliance governance of intelligent data center operations enabled by current AI technologies. These requirements can be grouped into the following categories: those related to data residency and sovereignty, privacy-by-design, data access controls, data protection through encryption in use and at rest, and auditability. Additional requirements include the management of user consent, data retention policies, and cross-border data movement.

Sovereignty refers to the right of a nation to govern itself without outside interference. The need for the sovereignty of data generated or stored in a jurisdiction has led to demands for the establishment of national data "borders," requiring organizations to store and process data on domestic IT infrastructure. As a result, several countries have enacted or proposed laws, such as the EU's General Data Protection Regulation (GDPR), that require specific types of data to reside on servers in the same country as its citizens. Depending on the jurisdiction, non-adherence to these requirements can lead to significant penalties, including severe reputational damage.

Many organizations have adopted privacy-by-design principles, which embed the consideration of privacy in every aspect of product design, across the architecture, technology, and development processes. Additionally, data owners require the ability to control who has access to their data and to restrict that access at different levels. Regulatory requirements usually require sensitive data to be protected both in use and at rest through encryption, and auditability of data access and transactions is also commonly required. Specific consent is often required before users' personally identifiable information (PII) can be used by AI systems. Moreover, the frequency and period over which consent can be sought is also guided by regulatory requirements. When data is accessed across borders, Data Protection Authorities (DPAs) recommend or require that extra safeguards, such as standard contractual clauses promoting data protection, be mandated.

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

Machine Learning	Risk Prediction	Threat Identification	Reduced Operational Risk
Deep Learning	Pattern Recognition	Security Intelligence	Faster Threat Detection
Time-Series Analytics	Predictive Monitoring	Failure Forecasting	Downtime Reduction
Autoencoders	Anomaly Detection	Compliance Violation Detection	Improved Reliability
Clustering Algorithms	Behavioral Analysis	Operational Monitoring	Resource Optimization
Reinforcement Learning	Adaptive Governance	Automated Decision Support	Dynamic Risk Mitigation

Table 3. AI Technologies for Intelligent Data Center Governance

5. AI Technologies Enabling Governance

Anomaly detection aims to discover (or label) observations that are significantly different (e.g., deviant, rare, or inconsistent) from the typical behaviour of the majority of observations. These atypical observations can be considered as unusual and may need to be investigated further. Predictive analytics refers to the forecasting of future events based on historical developments. Despite the differences in predictive and anomaly detection/labeling tasks, they are often performed with the same family of technologies: supervised or unsupervised learning models based on statistical methods or machine learning; or, when the time order of the data exhibits a significant aspect of the problem at hand, time series models. A combination of those methods is also possible. For anomaly detection, using labeled data — especially labelled anomalies — is preferable, but seldom possible. Thus, several methods for the same problems, unsupervised or semi-supervised ones, are proposed.

Anomaly detection and predictive analytics can be applied to all five risk types described above: operational, cyber, compliance, reliability, and supplier risks. However, each risk type requires a more specific description of the technology used. For example, concerning the data needed to apply a specific anomaly detection technique, the dimensions of the problem, the evaluation metrics of the results, and, especially, how the output should be integrated into the governance signals of the data center operations. The data requirements and evaluation metrics identified for the one risk type will differ from the requirements for the others.

Flow Chart 5: Intelligent Data Center Governance Platform

Governance Signal	Source Layer	Processing Method	Governance Outcome
Regulatory Signals	External Regulations	Policy Mapping	Compliance Enforcement
Operational Signals	Infrastructure Logs	AI Analytics	Incident Detection
Security Signals	Firewall & IDS Logs	Threat Intelligence	Cyber Risk Reduction
Vendor Signals	Supplier Platforms	Vendor Scoring Models	Vendor Reliability
Data Lineage Signals	Metadata Systems	Traceability Analytics	Audit Readiness

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

Governance Signal	Source Layer	Processing Method	Governance Outcome
SLA Signals	Service Monitoring Tools	Predictive Evaluation	Reliability Assurance

Table 4. Governance Signal Processing Framework

5.1. anomaly detection and predictive analytics

Anomaly detection and predictive analytics are among the AI technologies supporting integral governance. Their objective is to recognize patterns in business-as-usual operations and flag deviations, or anomalies, for further investigation. The anomalies considered are those arising from high-impact, low-incident events with business-continuity or data-sovereignty implications. Such events span operational outages, request processing anomalies, and policy/service compliance violations.

Operational anomalies are detected using unsupervised learning methods such as clustering, autoencoders, and one-class classifiers, and supervised methods with time-series or recurrent models. Risk to the data center's reputation and revenue requires that detection capabilities transcend its own operations, encompassing its interfaces with customers and third-party vendors as well. Therefore, such beyond-the-borders data are ingested and exposed en masse to enable the operation of specialized models. Data-processing actions are then taken based on anomaly explanations, for example, rerouting requests based on payment-authorization failures, while unexplainable detections trigger alerts for manual investigation.

Business-as-usual conditions pave the way for time-to-event predictions and the application of supervised methods for predicting outages and processing delays. Such supervised models are trained from data residing in the common data model and historical metadata storage. Production-environment fulfilment of model assumptions, mainly stationarity, is enforced via dedicated assessment and validation routines, potentially followed by supervised re-training with additional covariates supporting assumption relaxation. As abnormal patterns are detected, fulfillment of model assumptions is also monitored and fulfillment (or lack thereof) signalled to relevant model consumers. Such consumers be can alert handlers, for further interpretation of the warning, or resources responsible for recalibration of the anomaly detector.

Graph 3 — Data Sovereignty Compliance Radar: Compares GDPR vs. the OAS Privacy Framework across 7 dimensions highlighted in the paper: data residency, privacy by design, access controls, encryption, auditability, consent management, and cross-border transfers. GDPR leads in privacy-by-design and consent; OAS leads in cross-border transfer coverage.

6. System Architecture for Governance-Driven Operations

The system architecture for AI-driven enterprise risk management and compliance governance in intelligent data centers is presented as four integrated layers that form a conceptual data platform. The innermost layer comprises a wide array of data sources that generate data, events, and signals for governance. As a natural next step, the outermost layer includes governance components and solution microservices that rely on a variety of data for proper operation. The foundational data ingestion layer incorporates unified data, supporting a common data model with schemas,

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

semantics, and associated metadata that can be reused by different applications and data products.

Metadata management capabilities focus on data lineage and tracing to record the path of data from sources to consumers. Data interoperability and API governance facilitate data integration and exchange by enforcing compliance with a common data integration framework and establishing data contract requirements for data-sharing APIs. Furthermore, security and privacy-centric technical and organizational controls ensure protection of sensitive data throughout the data lifecycle.

The core data ingestion layer plays a pivotal role in enabling a multitude of governance signals. It comprises both traditional and nontraditional data sources, ready to be exploited by the various governance-driven components in the system architecture. Data provenance, lineage, and common metadata are essential requisites for AI-based enterprise risk and compliance management, underscoring the importance of a robust and effective data management framework for such a complex procedure. Data-driven solutions must support supervised and unsupervised anomaly-detection capabilities, as well as predictive analytics using classical and advanced machine-learning techniques.

Flow Chart 6: Continuous Compliance Monitoring & AI Operations

6.1. data layers and integration

Data sources include the full range of organizational systems, devices, tools, services, and applications producing, processing, storing, and consuming data or generating actions or output. Automated ingestion mechanisms feed data into the data platform pipeline. A common data model ensures consistency of concepts and terms across the organization, enabling reliable cross-analysis and integration of information from different sources.

Metadata management serves as a dynamic catalogue that contains details about the organisation's data, including associated business metadata (what types of data exist, in which system they reside, who is the data owner, how to access them, etc.) and technical metadata. With its active lineage tracing, the metadata management function integrates data lineage, provenance, and impacts analysis. It provides data dependency information for backtracking the origins of data, tracing their movement and transformations through the data ecosystem, and predicting which output might be affected when certain data elements change. Interoperability and API governance functions ensure that the content, quality, and security of APIs are addressed during their design and implementation, and that they comply with standards and specifications. Security and privacy understandability and condition-meeting requirements are built into the data platform architecture by design and monitored through governance signals.

Architecture Layer	Key Components	Functional Role	Governance Contribution
Data Source Layer	Sensors, APIs, Applications	Data Generation	Operational Visibility
Data Ingestion Layer	ETL Pipelines, Streaming Services	Unified Data Integration	Governance Signal Collection
Metadata Layer	Lineage & Provenance Systems	Data Tracking	Compliance Traceability

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

Architecture Layer	Key Components	Functional Role	Governance Contribution
AI Analytics Layer	ML & Predictive Engines	Risk Intelligence	Automated Governance
Governance Service Layer	Compliance Engines, Dashboards	Decision Support	Enterprise Governance
Security Layer	Encryption & Access Control	Data Protection	Regulatory Compliance

Table 5. Data Layer Architecture for Governance-Driven Operations

7. Conclusion

AI governance for intelligent data centers is an emerging cross-discipline that draws from information technology risk and compliance governance, machine learning operations, and corporate governance to advance intelligent data center operations as a governance, risk, and compliance stakeholder concern. Intelligent data centers must systematically mature and adopt AI-assisted enterprise risk and compliance governance solutions to comprehensively manage operational, cyber-resiliency, availability, regulatory, and vendor ecosystem risks and support compliance with the relevant data-management and privacy regulations, standards, and best practices.

An architecture for intelligent operations must support the application of data lineage, data provenance, and explainable AI techniques to internal operations and service delivery. Mapping enterprise risk and compliance considerations to an intelligent operational architecture and clearly aligning the data-residency, privacy, and security requirements of AI model training and operation with AI-assisted predictive maintenance bolsters defenses against operational, cyber-resiliency, and availability shortcomings. Well-defined and comprehensive signals for AI-assisted enterprise risk and compliance governance enable the wider intelligent data-center community to implement data-driven intelligent operations.

References

1. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115.
2. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 33–44.
3. Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. International Journal of Human–Computer Interaction, 36(6), 495–504.
4. Amistapuram, K. (2023). Privacy-Preserving Machine Learning Models for Sensitive Customer Data in Insurance

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

Systems. Educational Administration: Theory and Practice, 29(4), 5950-5958.
5. Ryan, M., & Stahl, B. C. (2020). Artificial intelligence ethics guidelines for developers and users: Clarifying their roles. HEC Forum, 32, 61–86.
6. Cihon, P. J., Maas, M. M., & Kemp, L. (2020). Should artificial intelligence governance be centralized? Design lessons from history. arXiv preprint arXiv:2001.03573.
7. Schneider, J., Abraham, R., Meske, C., & vom Brocke, J. (2020). AI governance for businesses. arXiv preprint arXiv:2011.10672.
8. Suresh, H., & Guttag, J. V. (2021). A framework for understanding sources of harm throughout the machine learning life cycle. Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 172–181.
9. Davuluri, P. S. L. (2023). AI-Augmented Sanctions Screening: Enhancing Accuracy and Latency in Real Time Compliance Systems. AI-Augmented Sanctions Screening: Enhancing Accuracy and Latency in Real Time Compliance Systems (December 15, 2023).
10. Raji, I. D., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 429–435.
11. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92.
12. Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. ACM Computing Surveys, 54(6), Article 115.
13. Inala, R. Designing Scalable Technology Architectures for Customer Data in Group Insurance and Investment Platforms.
14. Mökander, J., & Floridi, L. (2021). Ethics-based auditing to develop trustworthy AI. Minds and Machines, 31, 323–327.
15. Stix, C. (2021). Foundations for the future: Institution building for the purpose of artificial intelligence governance. AI and Ethics, 2, 463–476.
16. Gill, A. S., & Germann, S. (2021). Conceptual and normative approaches to AI governance for a global digital ecosystem supportive of the UN Sustainable Development Goals (SDGs). AI and Ethics, 2, 293–301.

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

17. Schmitt, L. (2021). Mapping global AI governance: A nascent regime in a fragmented landscape. AI and Ethics, 2, 303–314.
18. Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. Policy and Society, 40(2), 178–193.
19. Smuha, N. A. (2021). From a “race to AI” to a “race to AI regulation”: Regulatory competition for artificial intelligence. Law, Innovation and Technology, 13(1), 57–84.
20. Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 610–623.
21. Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2023). Toward AI governance: Identifying best practices and potential barriers and outcomes. Information Systems Frontiers, 25, 123–141.
22. Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. AI and Ethics, 2, 603–609.
23. Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. Government Information Quarterly, 39(4), Article 101685.
24. Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Putting AI ethics into practice: The hourglass model of organizational AI governance. AI and Ethics, 2, 627–636.
25. Weidinger, L., Mellor, J., Rauker, T., Griffin, C., Uesato, J., Huang, P.-S., Cheng, M., Glaese, A., Balle, B., Kasirzadeh, A., Kenton, Z., Brown, S., Hawkins, W., Stepleton, T., Birhane, A., Haas, J., Rimell, L., Hendricks, L. A., Isaac, W., … Gabriel, I. (2022). Taxonomy of risks posed by language models. Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, 214–229.
26. Yang, Z., Du, J., Lin, Y., Du, Z., Xia, L., Zhao, Q., & Guan, X. (2022). Increasing the energy efficiency of a data center based on machine learning. Journal of Industrial Ecology, 26(1), 323–335.
27. Yandamuri, U. S. (2023). An Intelligent Analytics Framework Combining Big Data and Machine Learning for Business Forecasting. Zenodo.

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 01 Issue: 01
RECEIVED: OCTOBER 19 REVISED: NOVEMBER 04 ACCEPTED: NOVEMBER 22 PUBLISHED: DECEMBER 08

28. Wang, Y., Li, Y., Wang, T., & Liu, G. (2022). Towards an energy-efficient data center network based on deep reinforcement learning. Computer Networks, 210, Article 108939.
29. Li, B., Wang, T., Yang, P., Chen, M., Yu, S., & Hamdi, M. (2022). Machine learning empowered intelligent data center networking: A survey. IEEE Communications Surveys & Tutorials, 24(4), 2521–2551.
30. Wang, S., Qin, L., Ma, C., & Wu, W. (2023). Research on overall energy consumption optimization method for data center based on deep reinforcement learning. Journal of Intelligent & Fuzzy Systems, 44(5), 7991–8004.
31. Brännvall, R., Gustafsson, J., & Sandin, F. (2023). Modular and transferable machine learning for heat management and reuse in edge data centers. Energies, 16(5), Article 2255.
32. Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., & Lundgren, M. (2023). The global governance of artificial intelligence: Next steps for empirical and normative research. International Studies Review, 25(3), Article viad040.
33. Batool, A., Zowghi, D., & Bano, M. (2023). Responsible AI governance: A systematic literature review. arXiv preprint arXiv:2401.10896.
34. Schuett, J. (2022). Risk management in the Artificial Intelligence Act. AI and Ethics, 3, 705–717.