



University of Wales
Trinity Saint David
LONDON

CLOUD ENGINEERING PRINCIPLES AND PRACTICE

Docker and AWS Cloud Implementation: A Technical and Analytical Study

Module: Cloud Engineering Principles and Practice (ACCA7027)

Student Name: Sameer Rajubhai Panchal

Student ID: 2516024

Table of Contents

1. Introduction.....	3
2. Literature Review: Security Frameworks and Models	3
2.1 Information Technology Infrastructure Library (ITIL)	3
2.2 ISO/IEC 27000 Family	4
2.3 Other Relevant Models and Frameworks	4
2.4 Comparative Analysis of Frameworks.....	5
3. Design of Security, Governance and Compliance Approach for NatureGreen (NG).....	6
3.1 Overview of Proposed Integrated Approach.....	6
3.2 Governance Structure.....	7
3.3 Risk Management Approach.....	8
3.4 Security Policies and Controls	9
3.5 Technical Protection Mechanisms	10
3.6 Contingency and Incident Response Planning.....	11
3.7 Compliance Requirements	12
3.8 Service Level Agreements (SLAs)	12
4. Critical Discussion: Importance of Updating Regulations and Standards	13
5. Conclusion	14
References.....	15

1. Introduction

Digital infrastructures, cloud services and connected systems, which are becoming a vital part of modern organisations, are a key element in ensuring the protection of information assets through data security, governance and compliance. NatureGreen (NG) is a worldwide health-oriented firm with massive wireless networks, cloud-based applications and vast internet presence as the demands of personal device usage among staff and consumers start increasing. Such circumstances increase the threats to sensitive information and intellectual property. This report issues a review of developed security frameworks and mouths out a systematic approach according to the needs of NG. Some of the assumptions are globally dispersed operations, division regulation and the use of third-party cloud providers. The report summarises the situation, discussion, suggested structure and critical analysis.

2. Literature Review: Security Frameworks and Models

2.1 Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) is one of the most used frameworks that offers systematic advice on how to offer quality IT services. ITIL is focused on integrating IT activities with the organisational goals with the assistance of the standardised processes, continuous improvement and clear management of the services. The fact that ITIL has gone through ITIL v3 to ITIL 4 indicates that it has embraced a transformational approach to the current digital environment, with agility, value co-creation and integrated service management practices being incorporated into the complex environment (Osakwe and Haitula-Waiganjo, 2025).

The ITIL Service Management lifecycle has its conventional five phases, including Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement. All these phases help organisations in establishing service value, designing resilient and safe services, executing change safely and continually ensuring improvement (Naik, 2023). The ITIL lifecycle diagram is a peculiar cycle and repetitive view of these stages, and puts a strong focus on constant feedback and constant improvement.

Within the environment of NatureGreen (NG), ITIL offers the planned processes of managing cloud services, wireless network systems and international service distribution. Its focus on service design underpins the secure architecture of a largely wireless network, whereas its advice on service transition improves change management of cloud adoption. The constant improvement processes in ITIL help NG perfect the processes involved in Bring Your Own

Device (BYOD), user support, incident management and service-level monitoring in distributed processes.

2.2 ISO/IEC 27000 Family

The ISO/IEC 27000 family includes global standards, which are aimed at helping in the management of information security. The ISO 27001 provides the specifications for the establishment of an Information Security Management System (ISMS), and the ISO 27002 gives best-practice advice in regard to the application of security controls. These standards are facilitated towards risk-based, systematic safeguarding of the information assets regardless of the diversity of the technology (Calder and Watkins, 2024).

ISO 27001 has a Plan-Do-Check-Act (PDCA) cycle encompassing the fact that the processes of information security develop according to the emerging threats and changes in organisations. The standard expects organisations to set the scope of the ISMS, identify risks to be identified, and apply suitable controls that are constantly monitored (Agarwal et al., 2023). The PDCA model facilitates resilience, adaptability and continuous improvement, which are essential elements for an organisation functioning in the volatile digital ecosystems.

ISO 27001 has annex A of 114 controls that are listed in domains including access control, asset management, cryptography, physical security, operations security, communications security and supplier relationships. Overall, these controls address threats that are related to the adoption of clouds, use of wireless networks and mobile devices (Dhruvitkumar, 2022). As an illustration, the secure access management is highlighted in Annex A.9, whereas an example of operations security practices is emphasised in the Annex A.12, like logging, monitoring and change management. Annex A controls can be presented in a tabular format to allow categorisation of each category of control in a more definitive way to organisational requirements.

In the case of NG, ISO 27000 provides a vital framework that can be used to safeguard intellectual property, client information, cloud computing and mobile access solutions (Islam, 2024). Its international presence facilitates its adherence to diverse regulatory settings, which is relevant in organisations that conduct their business towards international borders.

2.3 Other Relevant Models and Frameworks

NIST Cybersecurity Framework (CSF):

The NIST CSF is a risk-based approach to cybersecurity that is comprehensive and is broadly utilised by the public and private sectors. This structure is structured around five fundamental functions, namely Identify, Protect, Detect, Respond and Recover (Sun, Zhang and Fang,

2021). These operations together can aid in situational awareness, proactive protection, real-time monitoring, incident management and system recovery. The maturity levels and the adaptive controls offered by NIST are also appropriate for organisations that need an incremental security strategy in various infrastructures.

COBIT:

COBIT (Control Objectives on Information and related technologies) is concerned with the governance and enterprise IT management. It offers a methodical difference between aligning the IT objectives and organisational goals, as well as promoting risk management and compliance (Khan, 2022). Governance principles, performance metrics and capability models of COBIT enable the high-level oversight and hence apply to organisations that have the intention of developing mature and stable governance structures and that also govern the manner of accountability of all IT processes.

Zero Trust Security Model:

The concept behind the Zero Trust model is that of never trusting and always verifying (Simuni and Atla, 2024). It eliminates implicit trust in networks and implements tough identity checks, micro-segmentation, constant monitoring and high authentication protocols. Zero Trust is becoming more applicable in the setting that is typified by distantly connected access, cloud usage, and BYOD practices. Its granular control methodology is apt when dealing with distributed users and sensitive intellectual property in an organisation.

2.4 Comparative Analysis of Frameworks

Framework	Strengths	Limitations	Applicability to NG
ITIL	Strong service management structure; supports process maturity; enhances service stability and customer experience	Primarily service-oriented; limited technical security guidance	Useful for shaping cloud service delivery, wireless service management and support processes
ISO 27001/27002	Internationally recognised; provides comprehensive control catalogue; risk-based; compliance-focused	Requires significant resource investment for implementation and certification	Essential for protecting IP, customer data, cloud systems and BYOD environments

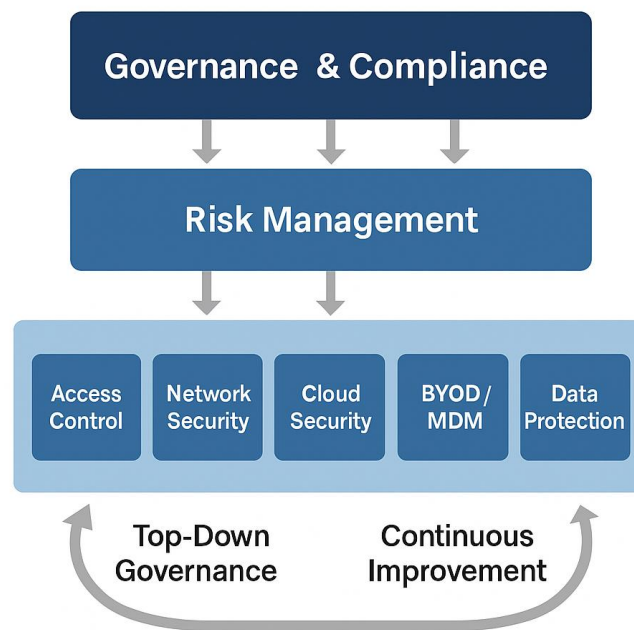
NIST CSF	Flexible, scalable, detailed security functions; strong emphasis on detection and response	Less compliance-driven; requires alignment with organisational structure	Supports continuous monitoring and incident response for NG's high-risk wireless and cloud environments
COBIT	Robust governance and accountability framework	Limited technical implementation detail	Helps NG establish governance structures and strategic oversight
Zero Trust	Strong protection for distributed networks; effective against modern threats; suitable for BYOD	Complex implementation; requires cultural and technical shifts	Highly relevant for NG's wireless network, cloud adoption and need to protect intellectual property

3. Design of Security, Governance and Compliance Approach for NatureGreen (NG)

3.1 Overview of Proposed Integrated Approach

The combined security, governance and compliance strategy of NatureGreen (NG) incorporates multiple globally accepted frameworks, risk-based decision-making, and the layered technical controls. The strategy establishes a consistency of structure that an organisation can use to provide secure operations in the cloud environment, wireless networks and globally distributed users (Salako et al., 2024). On a high-level design diagram, the governance would occur at the top of the design, which will be supported by risk management, to which operational security domains, which are access control, network security, cloud protection, monitoring and compliance management, are next.

This combined approach suits the strategic objectives of NG since it safeguards the intellectual property, increases customer and employee trust, complies with regulations and remains resilient in digital services. The strategy also supports secure digital innovation as it allows safe BYOD practices and cloud-based operations.



3.2 Governance Structure

There is effective governance that supports security and compliance. A well-defined governance framework allows accountability, management and coordination throughout the global operations of NG.

Security Governance Roles:

Chief Information Security Officer (CISO): Sees the strategic security direction, manages the ISMS, and maintains the alignment with the business objectives.

Data Protection Officer (DPO): Assures compliance with data protection regulations, supervises the privacy settings and administers rights of data subjects.

Security Operations Centre (SOC) Team: Oversees detectors, organises defence actions and response actions.

Compliance Officer: Manages regulatory ushering, in-house checks and outsourced evaluations.

Strategic Planning for NG:

The governance team outlines long-term security goals and puts them into perspective with the business strategy of NG, and dedicates resources to the most significant risks. Strategic planning is also a way to maintain uniformity in the applications of controls of cloud services, wireless networks, and international locations (Folorunso et al., 2024).

Policy Hierarchy:

Proper policy structure also increases levels of compliance and clarity.

Corporate Information Security Policy: Establishes the general security standards.

Acceptable Use Policy: Stipulates behaviour that is allowed on organisational systems.

BYOD Policy: Defines security settings as well as enrolment policies and surveillance on personal devices.

Data Classification Policy: Breaks down data into sensitivity levels, which dictate protection mechanisms.

Cloud Security Policy: Establishes obligations regarding communal cloud setup, encryption necessities and supplier control.

SECURITY GOVERNANCE STRUCTURE



3.3 Risk Management Approach

The risk management strategy of NG will be based on ISO 27005 and the NIST Risk Management Framework (RMF). The two methodologies focus on the identification of threats, vulnerability measures, the analysis of the risk, the treatment and continuous monitoring (Folorunso et al., 2024).

Example Risk Matrix:

The risk matrix of NG includes a customised risk categorisation in regards to likelihood and impact.

High Risk: Unsecured personal devices, improper configurations of the cloud, and weak wireless authentication.

Medium Risk: Staff abuse of intellectual property, lack of overseeing.

Low Risk: Hackings of physical access in restricted areas.

Key Risks Specific to NG:

BYOD Threats: Introduction of malware, data leakages, and unauthorised access.

Cloud Misconfigurations: Disclosure of confidential information, too many access privileges.

Wireless Vulnerabilities: Eavesdropping, rogue Access point and bad encryption (Onoja et al., 2021).

Insider Threats: Theft of intellectual property, unintentional release or violation of the policy. The risk treatment plans focus on encryption, endpoint management, Zero Trust architecture, improved monitoring, and compulsory staff training.

3.4 Security Policies and Controls

Operation controls and security policies conform to ISO 27001 and NIST CSF domains.

Access Control:

Centralised access and identity management(IAM)

Role-based access control (RBAC)

Sensitive system privileged access control.

Secure user identification and navigation.

Network Security (95% Wireless Environment):

WPA3 business-level encryption.

Guest, staff and IoT network isolation.

Intrusion detection and intrusion prevention (wireless).

Conducting a regular vulnerability scan.

Cloud Security:

Consolidated configuration foundations.

At-rest and in-transit data encryption.

Constant review of compliance.

Cross-cloud less privileged access control.

BYOD/Mobile Device Management (MDM):

Enforced registration of the devices.

Forced security profile (MFA, encryption, remote wipe)

Corporate and personal information is divided into containers.

Data Privacy and Protection:

Privacy controls that are GDPR-compliant.

Minimisation of data, breach notification and consent.

Ethical management of health-related information or behaviour information.

Monitoring and Incident Detection:

Centralised SIEM platform

Constant log examination and anomaly recognition.

Intelligence integration of threats.

3.5 Technical Protection Mechanisms

NG has a security architecture that implements various levels of defence.

Multi-Factor Authentication:

Enhances access control over cloud services, wireless systems, as well as remote access portals.

Encryption:

Encryption of messages between the endpoints.

High encryption of stored data.

Secured getting backups and Secure key administration.

Zero Trust Approach:

Authentication of all users and machines before access.

Lateral mobile prevention using micro-segmentation.

Program evaluation through constant sessions.

Endpoint Security:

Host-based behavioural analytics and firewalls, as well as anti-malware.

Patches and vulnerability fixes are automated.

Safe settings of both company-owned and personal computers.

Cloud Access Security Broker (CASB):

Gives visibility, control over access and policy implementation of various cloud environments.

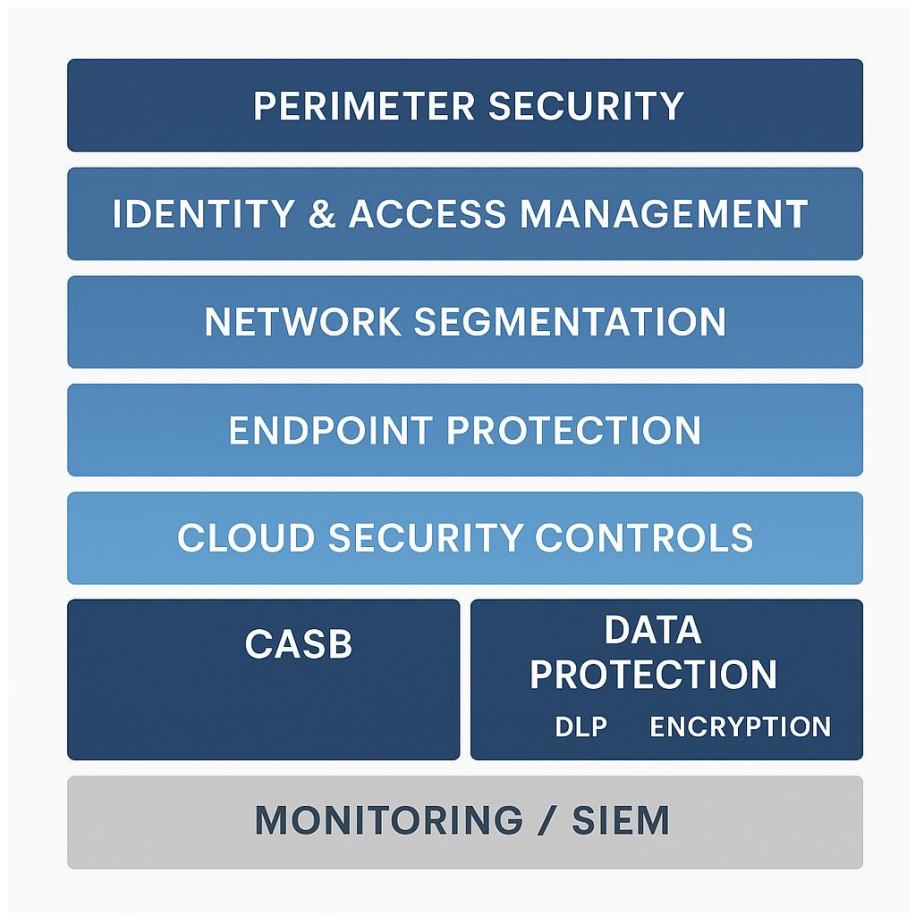
Intellectual Property (IP) Protection Controls:

Digital Rights Management (DRM).

Data Loss Prevention (DLP) mechanisms.

Stringent version control and getting a log of access.

The layered architecture diagram would conventionally show the perimeter controls, identity management and network segmentation and boundary controls with the cloud ending, endpoint protection and monitoring systems in combination.



3.6 Contingency and Incident Response Planning

A good contingency plan fortifies organisational resilience.

Business Continuity Plan (BCP):

Guarantees business continuity of key services even when other services go down, such as a cloud outage or other massive cyber-attack.

Disaster Recovery Plan (DRP):

Includes restoring IT systems, data recovery efforts, backup control and recovery time targets.

Incident Response Lifecycle (NIST SP 800-61):

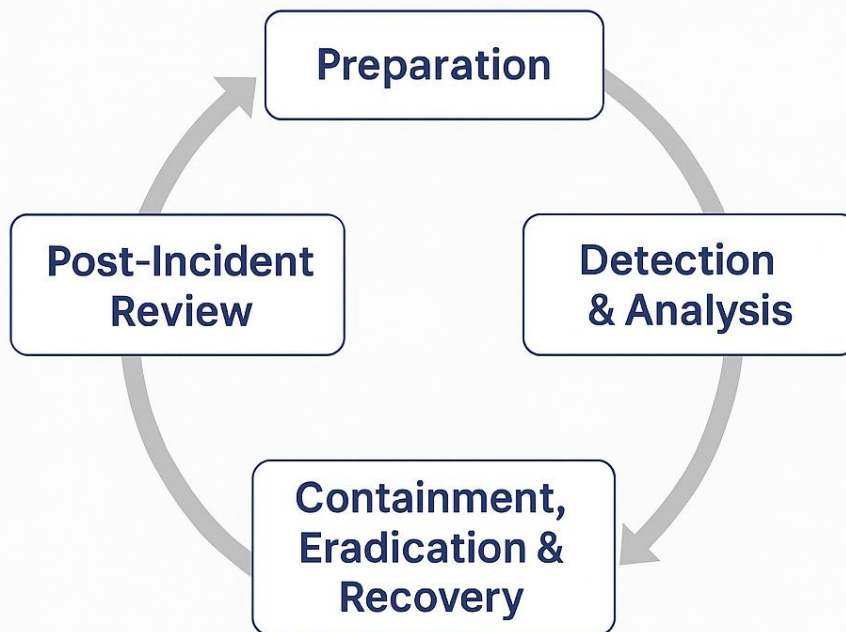
Preparation: Official policies, instruments, education and communication forms.

Detection and Analysis: Watching logs, notification triage, and incident classification.

Containment, Eradication and Recovery: Isolation of damaged systems, deletion and restoration of malware.

Post-Incident Activities: Learnings, control enhancements and policy renewals.

Incident Response Lifecycle (NIST SP 800-61)



3.7 Compliance Requirements

NG is an international company, and therefore, it is imperative to abide by several regulatory systems.

Key Regulations:

GDPR: Regulates the management of personal information in the EU.

HIPAA: Applicable to product data related to health in specific markets.

PCI-DSS: Necessary to process card payments.

Local Data Sovereignty Laws: Influence the data storage and transfer mechanisms.

A mapping of controls in the ISO 27001 and NIST models with particular legal requirements can be made, e.g., encryption to GDPR Article 32 sub-clause (a) or audit logging to PCI-DSS rules. Certain ethical aspects include responsible use of data, transparency and fairness in making data-driven decisions.

3.8 Service Level Agreements (SLAs)

SLAs specify relationships between NG and cloud service providers.

Key SLA Elements:

Performance: Response time guarantees, Uptime commitments.

Availability: Backup services, eventual availability.

Security Responsibilities: Practice of the shared responsibility model, timeline of incident reporting, and data handling procedures.

Compliance Obligations: It is certified using criteria like the ISO 27001 or the SOC 2.

Such clauses guarantee constant service provision and responsibility within the cloud ecosystem of NG.

4. Critical Discussion: Importance of Updating Regulations and Standards

The issue of sustaining proud security and compliance in a setting that is characterised by high-speed technological changes requires the implementation of constantly evolving regulations and standards. Cloud computing, artificial intelligence, the Internet of Things and the wide use of BYODs, organisational attack surfaces, and complex interdependencies among systems, devices and platforms have been introduced (Calder and Watkins, 2024). These advancements amplify the exposure to advanced cyber threats such as those of zero-day vulnerabilities, automated attacks and advanced persistent threats that capitalise on old-fashioned controls. In the absence of standards that are updated on a regular basis, organisations find it hard to keep up with alignment between security provisions and the latest threats.

Legal and ethical issues also support the necessity to evolve regulations on a regular basis. The current generation of consumers and other stakeholders demand increased protection of privacy as the digital footprints continue to grow with the number of interrelated services (Mahanti, 2021). Regulatory bodies should thus be flexible to provide fairness, transparency and accountability of processes in data processing, especially as AI empowered systems determine decisions made. Cross-border data flows also increase compliance complexity because organisations communicate with different jurisdictions, each with its own data protection requirements. New rules can be used to balance the expectations of companies, decrease ambiguity and create if and how global data transfers are allowed by law.

The improvement of standards regularly has great organisational payoffs. The revised models enhance the risk posture whereby the controls accommodate the existing vulnerabilities and not the past cases (Kuzio et al., 2022). When organisations adhere to current standards, they can demonstrate a commitment to being responsible data custodians, which will be competitive in markets where trust and reliability play a role in customer selection. Improved compliance practices also contribute to greater reputational standing, minimise regulatory fines, public outrage or long-term harm to the brand as a result of security breaches.

Nonetheless, it is problematic to comply with changing regulations. Making changes to standards can be a very expensive exercise with regard to finances and operation, particularly for organisations that are using the older systems that are not easily compatible with the modern-day controls. The cost of making infrastructure up-to-date, changes of policies and retraining personnel can be costly. Difficulty is also advanced by the necessity of regulatory changes to be interpreted and integrated into an existing operational process without breaking business flow (Pawar et al., 2024). Donations to change can be developed by employees or administrators, especially in cases where new demands introduce more restrictive ones or a change in the work process developed over time.

The need to maintain compliance also requires continued professional growth. The security and compliance staff have to constantly refresh their expertise to interpret new standards and implement the new best practices, and handle emerging technologies (Obioha et al., 2024). Unless the organisations engage in an ongoing learning process, they are likely to get the regulatory expectations wrong or implement ineffective controls. As a result, revising regulations and standards will be a strategic requirement, as well as an operational challenge that needs to be solved to guarantee secure operations in the long run.

5. Conclusion

The notion of security, governance and compliance is vital in protecting organisational resources in a digital world that is growing complicated. The widespread wireless network of NatureGreen, the use of the cloud globally and the increasing need to access the company using the smartphone (BYOD) pose an increase in vulnerability to cyber attack, regulatory risk and operational risk in operation. The identification of alternative frameworks facilitates the realisation of a coordinated and robust security model by incorporating known frameworks like ITIL, ISO 27001, NIST and Zero Trust principles. This method improves governance, promotes risk management and provides a secure utilisation of technical and procedural controls throughout the organisation. Constant check-ups, back-up plans and alignment of the compliance also strengthen securing the sensitive information and intellectual property. Technological landscapes are changing, and the constantly new regulations and standards are essential in keeping up with the current circumstances, effectively responding to the new threats and promoting ethical processes of data handling. All these measures will help NatureGreen to achieve operational resiliency, regulatory compliance and long-term confidence in its global stakeholders.

References

1. Agarwal, A., Kumar, S., Chilakapati, P. and Abhichandani, S., 2023. Artificial intelligence in data governance: Enhancing security and compliance in enterprise environments. *Nanotechnology Perceptions*, 19, pp.235-252.
2. Calder, A. and Watkins, S., 2024. IT governance: an international guide to data security and ISO 27001/ISO 27002.
3. Dhruvitkumar, V.T., 2022. Enhancing data security and regulatory compliance in AI-driven cloud ecosystems: Strategies for advanced information governance.
4. Folorunso, A., Adewa, A., Babalola, O. and Nwatu, C.E., 2024. A governance framework model for cloud computing: Role of AI, security, compliance, and management. *World Journal of Advanced Research and Reviews*, 24(2), pp.1969-1982.
5. Folorunso, A., Wada, I., Samuel, B. and Mohammed, V., 2024. Security compliance and its implication for cybersecurity. *World Journal of Advanced Research and Reviews*, 24(01), pp.2105-2121.
6. Islam, A., 2024. Data Governance And Compliance In Cloud-Based Big Data Analytics: A Database-Centric Review. *Academic Journal On Science, Technology, Engineering & Mathematics Education Учредители: All Academic Research*, 1(1), pp.53-71.
7. Khan, M.N.I., 2022. A Systematic Review of Legal Technology Adoption In Contract Management, Data Governance, And Compliance Monitoring. *American Journal of Interdisciplinary Studies*, 3(01), pp.01-30.
8. Kuzio, J., Ahmadi, M., Kim, K.C., Migaud, M.R., Wang, Y.F. and Bullock, J., 2022. Building better global data governance. *Data & Policy*, 4, p.e25.
9. Mahanti, R., 2021. Data governance and data management. Springer Singapore.
10. Naik, S., 2023. Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy. *The Eastasouth Journal of Information System and Computer Science*, 1(01), pp.69-87.
11. Obioha Val, O., Selesi-Aina, O., Kolade, T.M., Gbadebo, M.O., Olateju, O. and Olaniyi, O.O., 2024. Real-Time Data Governance and Compliance in Cloud-Native Robotics Systems. Oluwatosin and Kolade, Titilayo Modupe and Gbadebo, Michael Olayinka and Olateju, Omobolaji and Olaniyi, Oluwaseun Oladeji, Real-Time Data Governance and Compliance in Cloud-Native Robotics Systems (November 12, 2024).

12. Onoja, J.P., Hamza, O., Collins, A., Chibunna, U.B., Eweja, A. and Daraojimba, A.I., 2021. Digital transformation and data governance: Strategies for regulatory compliance and secure AI-driven business operations. *J. Front. Multidiscip. Res*, 2(1), pp.43-55.
13. Osakwe, J. and Haitula-Waiganjo, I., 2025. Data security and compliance through effective data governance. *International Journal of Information Security (IJIS)*, 4(1).
14. Pawar, A.S., Singh, N., Diwakar, M., Jadhav, S.B., Khalaf, O.I. and Lavate, S.H., 2024, June. AI-Enhanced Cybersecurity Governance and Compliance. In *International Conference on Frontiers of Intelligent Computing: Theory and Applications* (pp. 529-548). Singapore: Springer Nature Singapore.
15. Salako, A.O., Fabuyi, J.A., Aideyan, N.T., Selesi-Aina, O., Dapo-Oyewole, D.L. and Olaniyi, O.O., 2024. Advancing information governance in AI-driven cloud ecosystem: Strategies for enhancing data security and meeting regulatory compliance. *Asian Journal of Research in Computer Science*, 17(12), pp.66-88.
16. Simuni, G. and Atla, A., 2024. Hadoop in Enterprise Data Governance: Ensuring Compliance and Data Integrity. Available at SSRN 4982500.
17. Sun, L., Zhang, H. and Fang, C., 2021. Data security governance in the era of big data: status, challenges, and prospects. *Data Science and Management*, 2, pp.41-44.