

## **Task ‘Developing a Resilient and Strategic IT Framework’ Unit 11**

### **Introduction**

**CloudTitanPro** is a cloud, network, and security service provider dedicated to continually enhancing its operations to optimize resilience.

### **CloudTitanPro IT Governance and Risk Management Plan**

#### **One Identified Risk and Strategic Opportunity**

**RISK:** **CloudTitanPro** faces the risk of data breaches through its use of third-party vendors and supply chain, for instance, the support system provided by a vendor that processes user data that if breached, could impact client trust, reputation, and business continuity.

**OPPORTUNITY:** This presents a strategic opportunity to enhance trust by auditing and evaluating third-party vendors. This ensures liability in the contractual context, offering highly secure, resilient, and well-founded cloud services.

(Kolo, Joseph., Ogunmolu, Ejiofor, and Oyekunle, 2025)

### **Governance and Risk Mitigation Framework**

CloudTitanPro will establish organization-wide risk and governance processes that prioritize critical assets and are aligned with the business mission. These processes will be approved by executive leadership. Administrative and directive controls originate from top-down governance, as well as well-defined policies and incident response practices, such controls will help develop a security roadmap that aligns with the business mission and culture. CloudTitanPro will implement COBIT 2019 to ensure IT operations are aligned with objectives like uptime, reliability, customer satisfaction, and innovation. COBIT's five domains will guide the governance structure. In addition to strong Disaster Recovery (DR) effective strategy will support risk mitigation. The following strategy should include, for instance:

- Low-latency data replication across geographically distributed data centers and CDN technology.
- Regular DR drills and automated failover systems
- The Effective Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are derived from business impact analysis.

(Dionisius, Utama, 2023)

## **Compliance and Ethical Considerations**

CloudTitanPro needs to adhere to regulatory requirements, such as GDPR, HIPAA, ISO standards, and best practices IT, ethical guidelines, maintain effective practices in data handling and accountability mechanisms for instance ethics committees, ensuring integrity and client trust. To avoid discrimination and unfair, unethical

decisions, reduce the training of AI systems on biased or incomplete data. Ensure data integrity and limit exposure in breach scenarios.

(Ilochonwu, 2024)

## References

Ilochonwu, I.A., (2024). Information Technology Governance in Cloud Computing A Framework of Risk Management and Compliance. *IJIRT 170269 INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY*.

Dionisius, Y.B. and Utama, D.N., (2023). Evaluation of the Implementation of Business Continuity Management Using COBIT 2019 Framework in Public Sector. *Journal of System and Management Sciences*, 13(2), pp.409-427.

Kolo, F.H.O., Joseph, S.A., Ogunmolu, A.M., Ejiofor, V.O. and Oyekunle, S.M., 2025. Mitigating cybersecurity risks in financial institutions through strategic third-party risk governance frameworks. *Journal of Engineering Research and Reports*, 27(5), pp.173-193.

This document has been written solely for educational purposes. All references, names, and trademarks mentioned here remain the property of their respective owners and are used here strictly for the educational context. Grammarly was used exclusively for proofreading and enhancing the clarity and language of the text. All academic writing, analysis, argumentation, and conclusions are entirely the original work of the author.