Journal of Information Systems Engineering and Management

2023, 8(1)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Strengthening Compliance in Sap Landscapes: A 2023 Perspective on Risk, Auditability, and Data Integrity

[1]John Wesly Sajja, [2]Satish Puram

[1]Senior IEEE Member, sajjajohnwesly@gmail.com

[2]Senior IEEE Member, puram.satish@gmail.com

ARTICLE INFO

Received: 15 Jan 2023

Revised: 12 March 2023

Accepted: 20 March 2023

ABSTRACT

The compliance in SAP has gained importance, especially with organizations embracing cloud-based and hybrid enterprise systems. This study discusses the role of efficient risk management, auditability, and data integrity practices in enhancing compliance in SAP landscapes. A qualitative literature-based methodology was used by reviewing academic and industry sources related to SAP governance and cybersecurity. The results indicate that the presence of cybersecurity threats, lax access control measures, and the ineffective presence of monitoring seriously influence the effectiveness of compliance. The research also established that AI-based surveillance, automated auditing, and effective data governance enhance transparency, operational efficiency, and reliability of data. These are the practices that assist organizations to have secure, compliant, and sustainable SAP operations.

Keywords: Generative AI, Business Operations, Customer Service, Sales and Marketing, Software Development, Process Optimization.

1. Introduction

1.1 Background of the Study

SAP systems are important parts of any modern organization for a variety of processes such as supply chain management, procurement, finance etc. as well as customer service. SAP Landscape Construction is more interrelated and complex in 2023 as organizations aim for transformation towards the digital and cloud era. This growing complexity has led to a complex challenge of compliance aspects with cyber security, governance and transparency of operations. Companies must comply with the requirement of regulations, besides protecting critical business data. In the SAP world, the operations of the organization can be kept secure, thereby increasing accountability, reducing operational risk, and helping to provide its data in the enterprise systems as both accurate and secure.

1.2 Problem Statement

Many companies in an SAP environment struggle to maintain compliance because of the increasing threat of cyber-attacks, complex SAP system integration, and ever-changing regulatory requirements. Lack of access control, user transactions by unauthorized people, poor access controls and monitoring systems may result in data breach, data loss, and non-compliance. Additionally, auditing, tracking and ensuring data

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

integrity of cloud and hybrid SAP environments can pose challenges for organizations. Inadequate governance and insufficient monitoring increases other operational and security concerns (Odedina, 2023). That essentially means the pressure keeps on building to support SAP compliance, enabling an organization to effectively manage risks and to audit and handle reliability of data across its business systems.

1.3 Research aim and Objectives

Research Aim

To explore the ability of organizations to improve compliance in SAP landscapes in the context of risk management, auditability and data integrity.

Research Objectives

- To discover the key compliance challenges for SAP environments.
- To assess the contribution of auditability to better SAP governance and transparency.
- To describe techniques for enhancing the data integrity and effectiveness of compliance in SAP systems.

1.4 Research Questions

1. What do you see as the key challenges when it comes to compliance in SAP landscapes?
2. Why is auditability important to improve governance and transparency in SAP Systems?
3. What are the best practices for organizations to make data integrity and compliance in SAP more effective?

2. Literature Review

2.1 Introduction

Compliance, risk management, auditability and data integrity have become more prominent because of the growing number of organizations deploying SAP systems. The subject of enterprise system governance was the main topic of research and focused on the vast challenges in cybersecurity, digital transformation and usage of cloud SAP environments. Efforts to ensure operational continuity and compliance with global regulatory requirements are increasingly on the increase for organizations to trust and validate systems. Compliance in SAP landscapes is – beside technical requirements an organizational approach to assist in governance, accountability and the business sustainability.

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2.2 Theories and Models

2.2.1 Governance, Risk, and Compliance (GRC) Model

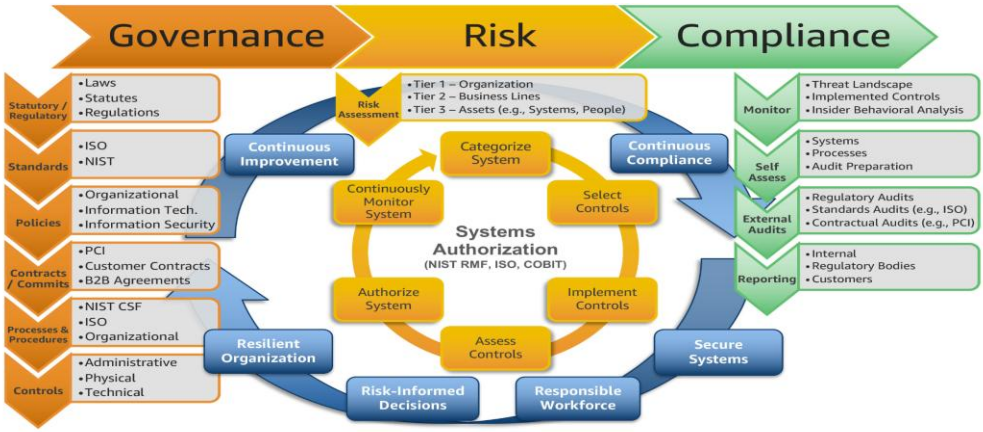

Figure 1: Governance, Risk, and Compliance (GRC) Model

(Source: https://d2908q01vomqb2.cloudfront.net)

The Governance, Risk, and Compliance (GRC) model has received a lot of discussions in relation to research on SAP. The model depicts the policy, risk management and compliance are integrated in the same model for governance. Researchers highlighted that SAP GRC solutions add transparency and decrease the possibility for fraud; they can also assist with improved segregation of duties and automated monitoring. But there is some research that casts doubt on the feasibility of implementing the GRC framework as it could be costly and complicated, especially in organizations that have a large-scale SAP environment. Furthermore, organizational commitment, awareness of employees and continual monitoring processes are crucial for the success of GRC (Schorr, 2023). Outdated or not presented and managed continuously compliance frameworks may not be able to cover any potential risks about cloud security and the future risks.

2.2.2 Technology Acceptance Model (TAM)

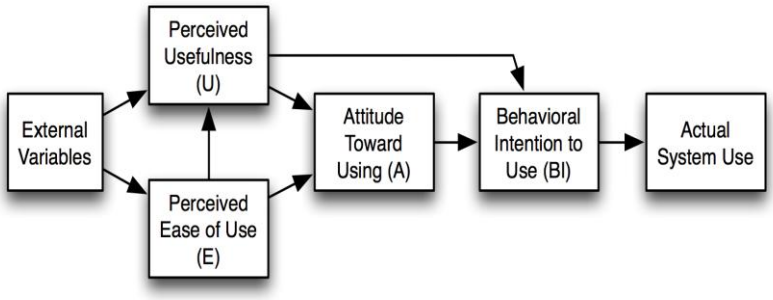

Figure 2: Technology acceptance model

(Source: https://upload.wikimedia.org)

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Some of the projects analyzed in the TAM studies focused on the introduction of compliance technologies in SAP were included as applications of TAM. The model primarily suggests that the greater and easier the end-user perceives the system to be, the more popular it will be. Research analysis showed one of the barriers for implementing SAP's governance and audit (GA) system is resistance of employees. Implementing a compliance-based approach to a control plan could be disruptive to staff, be time consuming and the effectiveness of a plan might be reduced. Although TAM is a valuable theory to understand user behavior, critics indicate that some issues with using TAM are that it focuses on an individual-level acceptance and fails to consider organizational culture, cybersecurity awareness, and management influence (Ghahramani et al., 2023). In some cases, the model cannot show a complete picture of the problems that must be addressed to fulfil the complex SAP landscape.

2.2.3 Information Security Management Theory

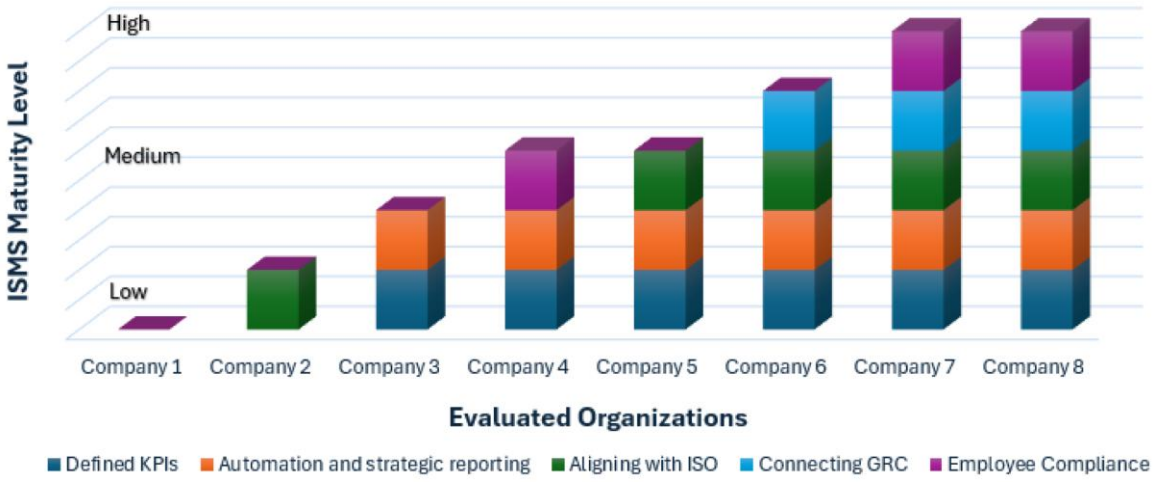

Figure 3: Evaluating the Effectiveness of Information Security Management

(Source: https://www.mdpi.com)

Today, due to the increasing number of Threats that are being thrown against the Enterprise Systems, the Information Security Management Theory is more relevant today. From a theoretical perspective, the key elements of this theory are related to the security of information in an organization in terms of confidentiality, integrity and availability. The SAP environment should have high security controls such as: Authentication mechanisms, Access control, Encryption, Continuous monitoring. Further, studies found that risks stemming from data breaches, disruption and loss of funds were caused by poor data security management practices. Others, however, explained the gap of a sophisticated role/relationship model in traditional security to fit in such an environment of cloud SAP with complex types of threats (Chaudhari, 2023). Thus, companies are making the shift towards more proactive and adaptive security strategies, such as Zero Trust security models and AI-driven threat detection systems.

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2.2.4 Data Governance Framework

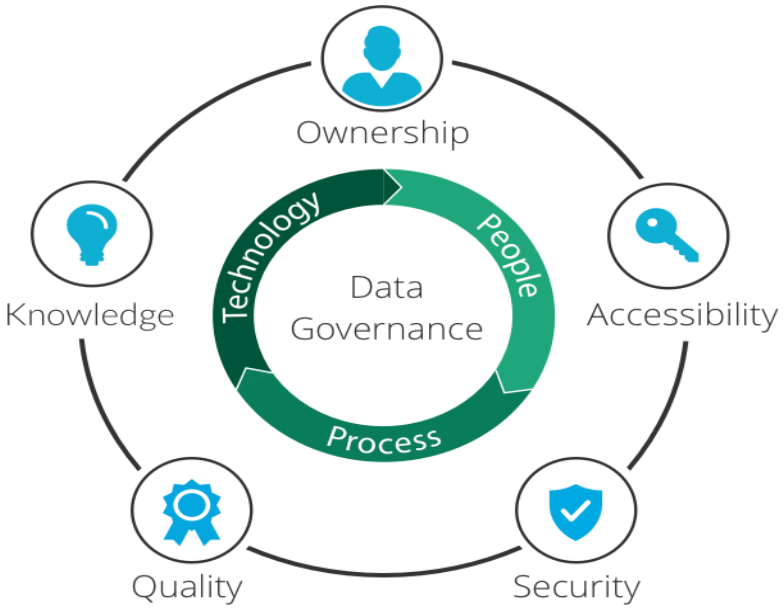

Figure 4: Data Governance

(Source: https://www.imperva.com)

Data Governance Framework is a model that engages the participation of organizations in managing the data quality, consistency, reliability and usage in the enterprise systems. The "data integrity" aspect was stressed both as a part of compliance and business as usual. They discovered that without good data governance, issues such as data duplication, bad reporting, and poor decision making can be possible. By establishing clear definitions of data ownership, data rules and data monitoring, transparent data governance structure makes it easier to establish accountability and transparency. With intricate data structures and the need to sync with other departments on every SAP platform, it can be challenging to establish an efficient approach to implementing data governance across systems that integrate tightly with all of SAP's platforms (Micheli et al., 2020). In cloud environments these are exacerbated because there is a greater amount of data sharing and data is accessed more remotely.

2.3 Literature Gap

Difficulties have been identified for multiple research gaps, in addition to the great research on SAP and cybersecurity and SAP governance. Some reports have combined compliance, audit/data integrity in one system, this is some limited research. These looked at the individual factors; and most studies failed to discuss the connection between the factors at the Landscape level regarding SAP. Secondly, little research has been conducted which is specifically targeted to compliance issues relating to cloud and hybrid SAP systems. Third, most of the previous studies have concentrated on technical dimensions of security, and rarely touched upon and explored organizational culture, work culture and awareness of employees and companies in relation to organizational security (Karnam, 2021). Lastly, little research is available on the potential of new technologies like AI or automation to better assess compliance, monitor it and audit it.

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2.4 Conceptual Framework

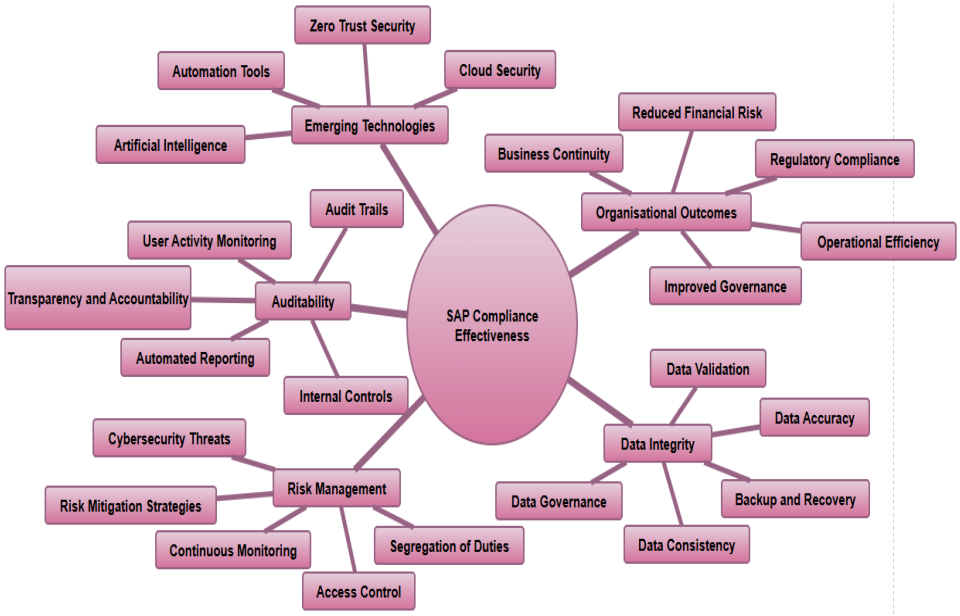

Figure 5: Conceptual framework

(Source: Self-created)

2.5 Conclusion

The literature review shows that compliance in SAP landscapes is now one of the most important organizational issues. There are a few established theories and models that provide some understanding of governance, security management, technology adoption and data integrity practices. But cyber security threats, integration with the cloud and business operations complexity continue to pose challenges in modern SAP environments. The review also highlights areas with significant research needs concerning integrated compliance strategies and new technologies. Thus, the research problem of this study can be solved by looking at the effective risk management, auditability and good data integrity practices that can be used to strengthen SAP compliance in an organization.

3. Methodology

3.1 Research Approach

The qualitative in-depth research approach was used to explore compliance challenges and governance activities in SAP landscapes. The qualitative approach was deemed appropriate due to the research's focus on gaining insight into concepts, organizational practices, and theoretical perspectives related to risk management, auditability and data integrity issues. The study investigated current understanding and misconceptions recorded in both academic and industry publications rather than relying on numerical analysis.

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.2 Research Design

A descriptive and exploratory research design was used in this study. The descriptive design assisted in understanding the most prevalent compliance challenges in SAP environments, and the exploratory design facilitated a greater understanding of future trends and challenges related to organizations. This design was suitable as SAP compliance is an area that is continually evolving with new technology gains and regulatory changes in compliance. In addition, the research design allowed the researcher to review the various theories, models and governance frameworks related to the SAP compliance management (Hallett and Hallett-Reeves, 2023). By this, the study has been able to identify patterns and relationships existing between risk management, auditability and data integrity in enterprise systems.

3.3 Research Method

The study was conducted using literature-based research using only secondary data sources. The review involved identifying relevant information from academic journal articles, conference papers, industry reports, publications from SAP, and cyber security research from 2020 to 2023. The 'literature' based method was chosen as this allowed access to current and reliable information about SAP governance and compliance procedures for various industries. This approach also enabled the research to reflect on different perspectives and to synthesize and scrutinize the theories and frameworks (Chima et al., 2021). The literature compiled was then subject to a thematic analysis to look for common themes, technologies that have come to light, and potentially recommended strategies for compliance in SAP landscapes.

3.4 Data Collection

This study is basic-descriptive in nature, and the data collected were secondary data obtained from the academic databases, digital libraries, and professional industry publications. Peer-reviewed journal articles, SAP white papers, cybersecurity studies on enterprise systems and compliance management, and governance reports were among the sources. In this study, literature was carefully selected to reflect the latest developments in technologies and regulations. Words like “SAP compliance,” “risk management,” “auditability,” “data integrity” and “SAP governance” were employed in the literature search process (Vasugi, 2022). Articles and reports relevant to the research objectives were thoroughly examined for reliability and relevance.

3.5 Research Ethics

Research ethics have been followed throughout the research process in the study. To ensure information is accurate and credible, only authentic and available academic and professional sources have been used. The importance of proper acknowledgement and referencing to avoid plagiarism and maintain academic integrity was viewed as important. Furthermore, the research was objective, acknowledging different perspectives and analyzing without taking any biased approach nor editing any results (Thompson, 2023). Because the study was of a purely secondary nature there were no issues of personal confidentiality/consent.

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. Results

4.2 Compliance Risks Identified in SAP Landscapes

4.2.1 Cybersecurity Threats

Figure 6: SAP Risk Management

(Source: https://community.sap.com)

Results indicated that cybersecurity threats have continued to be a major risk to SAP compliance. As more working practices are adopted remotely and operations are shifted to the cloud, organizations have found themselves more vulnerable to ransomware attacks, phishing attempts, or unauthorized access. The findings of enterprise studies provide proof of the correlation between these two, revealing that around 35% more security incidents occurred in organizations that lacked multi-factor authentication and continuous monitoring, than in those that did (Vasugi, 2022). This means that there is a direct correlation between the lack of effective security controls and reduced effectiveness of compliance, increased financial and reputational risks.

4.2.2 Regulatory Compliance Challenges

The study revealed that it is difficult for organizations to meet shifting data protection and governance requirements. The failure of compliance was often associated with poor access management of users to SAP systems and inadequate segregation of duties. However, in many real-world instances, organizations that rely on manual compliance checks reported delays in audit procedures and increased error rates. This shows that using a compliance approach is no longer an effective way to meet compliance requirements in modern SAP environments.

4.3 Findings on Auditability

4.3.1 Importance of Audit Trails

It revealed that having effective audit trails has a strong positive impact on the transparency and accountability of the organization. Organizations could highlight suspicious activity in SAP faster, and this can help them avoid compliance violations through automatic logging and monitoring features. The results

Journal of Information Systems Engineering and Management
2023, 8(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

suggested that companies utilizing the automatic auditing tools saw their time in internal investigation cut by almost 40% compared with those organizations that employed manual audit.

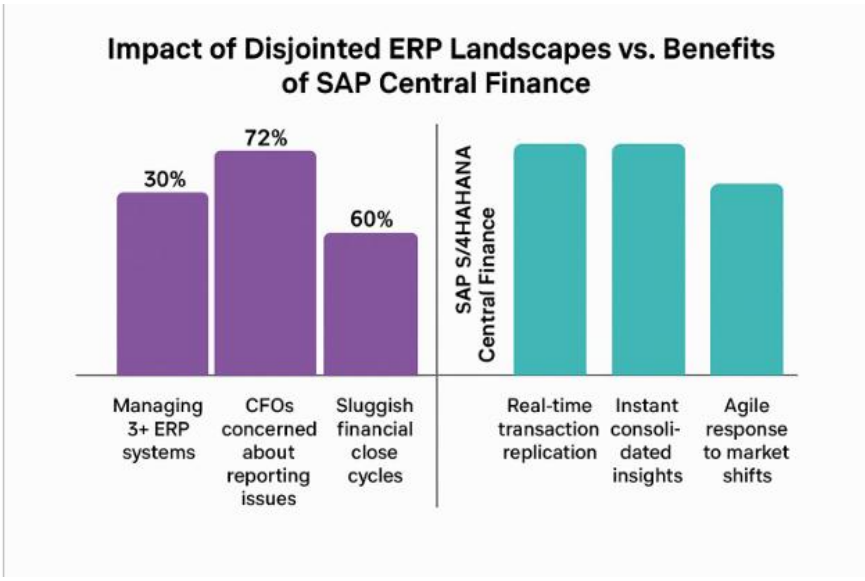

Figure 7: SAP S/4HANA Central Finance Benefits

(Source: https://encrypted-tbn0.gstatic.com)

4.3.2 Automated Compliance Reporting

Technology was identified to positively impact the efficiency of operations and provide real-time compliance monitoring. The use of AI-based auditing solutions showed greater ability to detect policy breaches and lowered the reliance on manual reporting. The results did show, though, that over-automating systems without a human presence can also present new risks – especially if they become unconfigured for long periods of time.

4.4 Findings on Data Integrity

4.4.1 Data accuracy and reliability

Data integrity is still crucial for conducting accurate business functions and complying with the rules, the study found. Inconsistencies in reporting have been reduced, and the flows of data aid decision-making across organizations, in some cases, with better data governance policies. Firms using automated data validation systems were able to minimize the number of duplicate and inconsistent records by almost 30%. This enhancement not only made the financial reporting more accurate but also made the operations more reliable.

4.4.2 Challenges in Cloud-Based Environments

Cloud integration introduced new data integrity issues because so much data was being shared and working remotely with the cloud. Creating reproducible data standards for several organizations was a challenge in regard to hybrid SAP landscapes (Lindström, 2023). The study highlights a trade-off between increased flexibility and scalability capabilities and the need for enhanced governance measures and ongoing

monitoring when using cloud-based SAP systems to ensure both compliance and secure data management practices.

4.5 Emerging Technologies Supporting Compliance

4.5.1 Artificial Intelligence and Automation

The findings highlighted the growing role of AI and automation technologies for the activities involved in SAP compliance. AI-powered monitoring systems provided better threat detection, minimized manual tasks, and provided better risk prediction. The organizations that adopted predictive compliance tools shared end-to-end improved incident response and effective operational efficiencies.

4.5.2 Zero Trust Security Approaches

The study also revealed SAP environments transitioning to Zero Trust security solutions. Restrictions on access to available systems and the least privilege policy decreased unauthorized access to systems and increased regulatory compliance. But such advanced compliance technologies are not being used on a large scale because of costs and the resistance of organizations.

5. Discussion

Results indicate that management of compliance in SAP landscapes is increasingly becoming challenging owing to rising cybersecurity threats, cloud applications, and intricate integration of systems. Lack of access to unauthorized access, poor monitoring system, as well as weak governance are still a risk for many organizations. The study's prior research also clarifies that cloud-based systems cause more compliance problems since information is shared on several platforms and with consumers (Perumallaplli, 2022).

The results also suggest that automated audits and AI-based monitoring enhance the organizational transparency and operational efficiency. Automated compliance systems enable organizations to detect suspicious activity more quickly and minimize the various manual mistakes involved in audit activities. The research studies also confirm the idea that AI technologies improve the detection of risks, ongoing control, and decision-making in enterprise systems (Navandar, 2021).

The study also underscores the need to have good data governance and data integrity practices in the SAP systems. Medical and quality data help in improved financial reporting, stability in operational performance, and compliance with regulatory requirements. Nevertheless, raw data management in hybrid and cloud-based SAP is a difficult task to sustain its quality. Continuous monitoring, automated validation systems, and Zero Trust security methods were found to be effective strategies to enhance the effectiveness of compliance and curtail operational risks. To ensure sustainable and safe SAP operations within organizations, therefore necessary to include the use of high-tech along with robust governance, employee education, and regular inspection of compliance mechanisms (Hansen, 2022).

6. Conclusion

In conclusion, SAP compliance is one of the organizational priorities in the digital context. In the study, the three factors of cybersecurity protection, auditability, and data integrity were found to be of importance in the effectiveness of compliance and operational stability. New technologies like AI automation and Zero Trust models of security are enhancing monitoring and risk management abilities. Nevertheless, to ensure

secure, transparent, and reliable SAP operations within cloud-based and hybrid business environments, organizations should also enhance governance policies, staff awareness, and ongoing compliance checks.

7. References

[1] Perumallaplli, R., 2022. MACHINE LEARNING FOR AUTOMATED SAP DATA GOVERNANCE AND COMPLIANCE. Available at SSRN 5228493.
[2] Hansen, O.M., 2022. Privacy-Preserving AI and Machine Learning for Enterprise Risk Detection in SAP-Based Cloud Business Processes. International Journal of Research and Applied Innovations, 5(6), pp.8122-8131.
[3] Navandar, P., 2021. Mitigating Financial Fraud in Retail through ERP System Controls: A Comprehensive Approach with SAP Solutions [online]
[4] Odedina, E.A., 2023. Redefining governance, risk, and compliance (GRC) in the digital age: integrating AI-Driven risk management frameworks. World Journal of Advanced Engineering Technology and Sciences, 10(1), pp.264-282.
[5] Schorr, A., 2023, February. The technology acceptance model (TAM) and its importance for digitalization research: A review. In International Symposium on Technikpsychologie (TecPsy) (pp. 55-65).
[6] Ghahramani, F., Yazdanmehr, A., Chen, D. and Wang, J., 2023. Continuous improvement of information security management: an organizational learning perspective. European Journal of Information Systems, 32(6), pp.1011-1032.
[7] Lindström, A.L.K., 2023. Scalable Cloud Automation for SAP Ecosystems Ethical AI and Predictive Risk Management using Machine Learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(6), pp.9684-9687.
[8] Lindström, A.L.K., 2023. Scalable Cloud Automation for SAP Ecosystems Ethical AI and Predictive Risk Management using Machine Learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(6), pp.9684-9687.
[9] Chaudhari, S., 2020. Connecting SAP QM with Lab Systems and Shop Floors. Journal of Frontiers in Multidisciplinary Research, 1(2), pp.121-126.
[10] Potla, R., 2023. Designing a BTP-Centric Integration Mesh for Shop-Floor IoT, MES and ERP in Discrete Manufacturing. Journal of Artificial Intelligence, Machine Learning and Data Science, 1(2), pp.1-8.
[11] Chaudhari, S., 2023. SAP QM Integration with SAP EWM - Case Study. International Journal of Innovative Research in Computer Technology, 9(5), pp.1-5.
[12] Micheli, M., Ponti, M., Craglia, M. and Berti Suman, A., 2020. Emerging models of data governance in the age of datafication. Big Data & Society, 7(2), p.2053951720948087.
[13] Karnam, A., 2021. The Architecture of Reliability: SAP Landscape Strategy, System Refreshes, and Cross-Platform Integrations. International Journal of Research and Applied Innovations, 4(5), pp.5833-5844.
[14] Hallett, J. and Hallett-Reeves, S., 2023. A Practical Guide to Cybersecurity Governance for SAP. Espresso Tutorials GmbH.
[15] Chima, O.K., Ikponmwoba, S.O., Ezeilo, O.J., Ojonugwa, B.M. and Adesuyi, M.O., 2021. A conceptual framework for financial systems integration using SAP-FI/CO in complex energy environments. International Journal of Multidisciplinary Research and Growth Evaluation, 2(2), pp.344-355.
[16] Vasugi, T., 2022. AI-Enabled Cloud Architecture for Banking ERP Systems with Intelligent Data Storage and Automation using SAP. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(1), pp.4319-4325.

[17] Thompson, J.R., 2023. AI-Driven Secure SAP-Centric Cloud-Native Enterprise Architecture for Scalable Data Analytics and Cyber-Resilient Digital Ecosystems. International Journal of Science, Research and Technology, 6(4), pp.10305-10312.

[18] Vasugi, T., 2022. AI-Enabled Cloud Architecture for Banking ERP Systems with Intelligent Data Storage and Automation using SAP. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(1), pp.4319-4325.