International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue:11 | Nov-2021 SJIF Rating: 6.714 ISSN: 2582-3930

SAP Security Strategies for Data Ring-Fencing in Mergers and Acquisitions

Gururaj K Y

Introduction

Consolidating separate IT infrastructures can lead to increased risks to confidential information, broadening the overall attack surface. APIs and data pipelines connecting cloud platforms can even lead to inadvertent disclosures. Thus, robust access controls are critical during IT integration, especially in highly sensitive or regulated environments.

Static controls are typically not enough to manage the complexity and volatility of IT integration, especially during an M&A deal when personnel and process requirements can be in a state of flux. This is where dynamic access controls play a critical role in managing and governing collaboration and use between enterprises.

Ring-fencing data in SAP can be used to segregate sensitive business data during merger and acquisition (M&A). This approach entails stringent user identification and Role-Based Access Control for effective data segregation. These controls help to avoid accidental sharing of strategic plans or other IP with unauthorized users.

Literature Review

IS literature emphasizes the importance of identifying the right theoretical model to cope with integration-related challenges, especially in the context of M&A. The discussion revolves around overcoming the fragmented character of the extant literature and advancing a holistic view on the integration-related risks and challenges. However, a gap exists as it fails to address the granular challenges associated with SAP integration, especially when it comes to security. Therefore, further research is necessary to fill this gap and provide insights into the most efficient means of ring-fencing SAP data and ensure that these strategies are effective in minimizing risks during ERP integration. For example, although the DySIIM model presents an interesting contribution to the debate as it considers integration as a multi-facetted managerial challenge that goes beyond technical compatibility, it would be interesting to operationalize such models in order to develop efficient means of integration management that take into consideration the need for siloing SAP data. Similarly, literature on IT carve-outs sheds light on the complex processes involved in carving-out IT landscapes but fails to consider the complexity of integrating SAP landscapes especially when security is a priority. Further research is thus called for.

In the context of multi-cloud ERPs, the Zero Trust concept of micro-segmentation is a paradigmatic example. It offers a means of addressing the challenge of user access in distributed systems where traditional, perimeter-based security falls short. Zero Trust minimizes the attack surface and implements granular, identity-based controls that follow least-privilege principles.

Managing user access in multi-cloud ERPs can benefit from identity brokering and federation, which can be used to centralize identity management and streamline the authorisation process without compromising agility. Federation facilitates trust among various parties, including cloud, on-premises, and identity providers, through protocols such as SAML, OAuth, X.509 to eliminate the need for replicating user credentials. However, in order to ensure data ring-fencing, identity federation alone may not be enough, especially in situations where organisations have different identity management policies. The challenge lies in understanding and aligning authorisation rules and roles that differ between the two organisations. Different meanings may be attributed to attributes, such as roles and entitlements, within the organisation. Authorisation decisions require reconciliation of attributes at runtime based on the user's organisation and access context, such as the purpose of access, sensitivity of the requested resources, and temporary collaboration between the two organisations. It is important to monitor and control data access between SAP landscapes through fine-grained authorisation controls, identity federation, automated provisioning/deprovisioning, comprehensive logging, periodic access reviews, etc. This ensures that access is restricted and documented and that users have access to the minimum necessary data to carry out their responsibilities, thereby facilitating compliance with internal and regulatory requirements.

However, although policy-as-code is presented as an interesting contribution, there is a gap as it fails to address the question of how a codified security policy adapts to changes in authorisation boundaries especially in the context of multi-cloud ERPs. Further research is called for and longitudinal empirical research might yield interesting insights.

Methodology

In addition, the research follows a design science approach, which is particularly apt when abstract requirements have to be formulated into technical solutions. Based on a set of requirements, a solution is developed and refined by the iterative application of the proposed solution to the problem at hand. This way, design science research emphasizes artifact-centricity and novelty.

How does this translate into our research? To address this, we provide a comprehensive overview of the components that comprise SAP data ring-fencing as well as the interaction between them. For this purpose, we draw upon a multi-vocal literature review, that is, a special form of systematic literature review, which aggregates and analyzes scientific literature in addition to industry sources such as best practice frameworks or white papers to develop a holistic understanding of a highly applied field such as security orchestration. Next, we aim to develop criteria to evaluate the effectiveness and efficiency of data ring-fencing solutions, which is realized through expert-based, semi-structured interviews to capture state-of-practice requirements. Finally, we suggest how these criteria can be applied to SAP-specific data ring-fencing solutions.

To address these challenges, CIOs need a set of criteria to evaluate SAP data ring-fencing solutions and services. This way, they can select the right combination of technical and organizational measures to protect confidential data in multi-tenant systems. Criteria should capture technical properties of ring-fencing solutions such as granularity , efficiency such as the speed at which access control policies are enforced across tenants, and auditability, that is, the extent to which solutions provide meaningful insights into user activity through access control logs. However, they should also reflect organizational factors like user acceptance and perceived usefulness. For example, policy mining techniques can be used to gain insights into the actual application of privileges to understand how often permissions are exercised. To get a sense for the impact, this information is related to the amount of data that has been created or modified. The goal is to understand how permissions are used in reality.

Once such a list of requirements is determined, it is possible to apply them to solutions for data ring-fencing in SAP and determine gaps or strengths. For example, diverging access control policies, roles, and processes can be analyzed along organizational hierarchies and compared to state-of-the-art such as ISO 27001 to identify gaps in access control policies, processes, or practices. In addition, technical controls such as data classification schemes or identity federation approaches can be assessed to identify gaps with regard to trust-building activities. Finally, ring-fencing solutions need to adhere to legal frameworks like GDPR to ensure that privacy-by-design is upheld throughout the reconciliation of IAM solutions. This way, we can propose solutions for data ring-fencing that allow for the reconciliation of SAP-based ERP solutions while safeguarding sensitive information in M&A processes, but do not interfere with business-as-usual activities of subsidiaries.

Results

Another important aspect of ring-fencing is whether to implement a standardized SAP solution provided by the acquirer for the target or keep existing solutions. Standardization of IT infrastructure may facilitate separation by enforcing policies and reducing the delay in audits and thereby enhancing the accuracy of reporting. Moreover, an integrated SAP solution can improve the success of M&A by providing a complete and up-to-date view of business processes after M&A. On the other hand, in case of different SAP solutions or ERP systems, ring-fencing of SAP environments will be more challenging. Data validation, segregation of administrator's duties, and monitoring of interfaces will be crucial aspects that require enhanced security to facilitate separation. In addition, an integrated solution has many benefits compared to interfaced solution. Data integrity, timely and complete information, and user's efficiency can be enhanced by minimizing or eliminating interfaces among applications. However, implementation of an integrated solution may require considerable amount of time and resources to consolidate current solutions. Hence, companies should carefully assess the benefit of standardization before implementing a common ERP system.

The success of SAP ring-fencing is crucially dependent on effective and efficient governance for separation. It requires a comprehensive understanding of SAP applications, security, data flows, business processes, local practices, and compliance requirements across country boundaries. However, theoretical solution is not always practically implementable considering limited compatibility among solutions. Moreover, SAP ring-fencing requires more than a solution, an action plan, and team. Preparation plays a key role in facilitating separation in addition to hybrid team with relevant skills. Ring-fencing is more likely to be successful if the company develops a risk-based approach rather than standardization. By focusing on key business objectives and linking them with SAP security, a company can become more resilient to changes. Ring-fencing of SAP environments requires the balance among IT's continuous operations and enhanced security.

Separation is more than IT's technical exercise. Ring-fencing requires comprehensive understanding of business goals, processes, and relevant SAP solutions. It is crucial to develop an approach based on organizational and environmental context to facilitate separation. This can be accomplished through enhanced data classification and automated governance to address the complexity across country boundaries.

Discussion

Static and homogeneous access controls do not allow for diverging integration goals between various departments. Thus, it is essential that IT and SAP admins consider how SAP is used within the context of integration and divestment and apply controls accordingly.

Segregation of Duties in SAP reduces the likelihood of compliance and audit challenges caused by accessing data in other systems. Inconsistencies between systems make it harder to establish controls and can lead to an over-reliance on compensating manual controls, which can lead to security and governance challenges within an organisation. Automation tools help to minimise vulnerabilities within heterogeneous systems. Machine learning can offer real-time identification of anomalous behaviour and predictive analysis to understand potential risks to block unauthorised access between organisational boundaries.

Separating IT during a carve-out or divestment process can present a number of challenges around compliance, increasing an organisation’s risk of regulatory breach, as well as increased costs around auditing. Increased organisational complexity during M&A has been linked to an increased frequency of data breaches, especially in cases where organisations operate within different industries or business areas. Establishing clear lines of ownership and accountability transforms security policies into a governance structure, and can be used to ensure that security is enforced, not just documented. Aligning operational security can help to overcome any inconsistencies between target and acquirer systems.

In the context of SAP, ring-fencing is about establishing controls to ensure that temporary measures don’t create permanent risks and reduce excess access across organisational boundaries. However, it is important to view ring-fencing not just as an access management or SAP-specific challenge but also a governance issue that requires continuous monitoring of SAP authorisation and roles, privileged credentials, data flows and interfaces between systems. Changes to organisational complexity impact controls around users, technologies and processes.

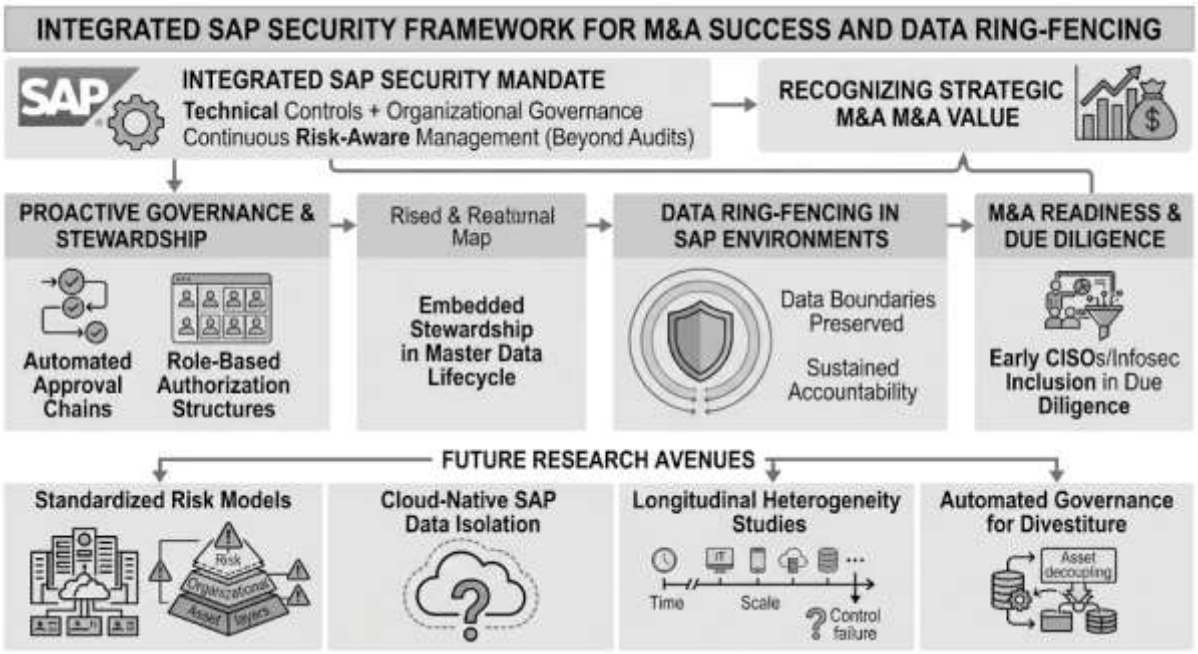
From a SAP-specific perspective, this means that ring-fencing needs to be considered during due diligence, integration, TSA’s and stabilisation phases, and should be monitored consistently during this time.

Conclusion

Further research should address the impact of cloud-native SAP solutions on data segregation and system perimeters. Also, as companies increasingly leverage SMACIT technologies, standardized cybersecurity risk modeling can help researchers to link technical configurations and organizational complexity. Longitudinal research can explore how agile SAP security strategies affect the frequency of integration challenges in heterogeneous IT landscapes.

Integrating security considerations during the early phases of the M&A process can contribute to deal success. Evidence indicates that companies that actively include information security leaders in the due diligence process experience higher M&A success. Effective SAP security entails a combination of technical and organizational controls that extend beyond

periodic audits. Creating an incentive-compatible modular SAP security concept can be helpful after mergers as it can be used as a blueprint for other M&A deals. Automating the SAP security concept can facilitate governance. For example, approval processes can be configured into SAP, embedding the notion of stewardship in master data management processes. Role-based access control is another example where governance is built into the system. This approach to SAP security not only can help companies better manage the challenges of SAP security during M&A, it also can facilitate divestment by ensuring that IT can be securely decoupled. Embedding governance in SAP can facilitate stewardship of SAP. Ultimately, a more holistic and proactive approach to SAP security can prevent data perimeters from becoming a source of lasting vulnerabilities during M&A.



References

Bloch, F. (2020). Impact of corporate audit findings on the planning and implementation of SAP ERP Segregation of Duties in a corporate environment. In *Theseus (Ammattikorkeakoulujen)*. https://www.theseus.fi/handle/10024/349394

Bodipudi, A., & Gopireddy, R. R. (2021). Implications and Strategies of Cyber Threat Landscape in Hospital Mergers and Acquisitions. *International Journal of Science and Research (IJSR)*, *10*(10), 1632–1636. https://doi.org/10.21275/sr24801082224

Henningsson, S., Yetton, P., & Wynne, P. J. (2018). A Review of Information System Integration in Mergers and Acquisitions. *Journal of Information Technology*, *33*(4), 255–303. https://doi.org/10.1057/s41265-017-0051-9

Hjerppe, K., Ruohonen, J., & Leppanen, V. (2019). The General Data Protection Regulation: Requirements, Architectures, and Constraints. *arXiv (Cornell University)*, 265–275. https://doi.org/10.1109/re.2019.00036

Hosseini, K. D., & Paul, D. L. (2017). Assessing Cybersecurity Risk for Oil & Gas Mergers and Acquisitions. *SPE Western Regional Meeting*. https://doi.org/10.2118/185626-ms

Hough, J. R., Haines, R., & Giacomo, S. D. (2007). Contextual factors affecting the integration of enterprise systems in post-merger oil and gas companies. *Enterprise Information Systems*, *1*(4), 421–441. https://doi.org/10.1080/17517570701630404

Tanriverdi, H., & Du, K. (2009). DISINTEGRATING INFORMATION TECHNOLOGY IN CORPORATE DIVESTITURES : IMPLICATIONS FOR REGULATORY COMPLIANCE RISKS AND COSTS. *International Conference on Information Systems*, 50. http://dblp.uni-trier.de/db/conf/icis/icis2009.html#TanriverdiD09

Tanriverdi, H., & Du, K. (2020). Corporate Strategy Changes and Information Technology Control Effectiveness in Multibusiness Firms. *MIS Quarterly*, *44*(4), 1573–1617. https://doi.org/10.25300/misq/2020/14223

Yamsani, N. (2021b). Governance by Design: Secure Role Delegation and Approval Structures in Enterprise Master Data Systems. *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.5281/zenodo.18296976