ISSN: 2633-4828 Vol. 3 No.2, December, 2021

International Journal of Applied Engineering & Technology

GOVERNANCE AND COMPLIANCE IN SAAS IMPLEMENTATIONS: A SERVICENOW-CENTRIC MODEL FOR PCI, GDPR, AND SOX READINESS

Venkata Subramanya, Sai Kirana and Vedagiri
Sr Software Developer & Architect
(Independent Researcher)
Rackspace Cloud Services, San Antonio, Texas, USA
vvsskiran@gmail.com
orcid - 0009-0002-6760-8099

ABSTRACT

The growing use of Software-as-a-Service (SaaS) platforms provided difficult regulatory issues to companies with the mandatory use of the PCI-DSS, GDPR, and SOX guidelines. This paper has investigated the usefulness of a ServiceNow-based governance and compliance model that aims at improving regulatory preparedness, audit transparency, and risk management maturity. The mixed-method method was employed to collect data in three organizations in BFSI, healthcare and IT services industries based on interviews, surveys, workflow observations and audit documentation reviews. Those findings showed that the compliance maturity significantly increased, and the organizations showed more than 40% improvement in compliance scores, as well as nearly 47% decrease in the time of the audit cycle after the implementation. Accountability was greatly enhanced through centralized audit evidence repositories and automated control mapping, real-time dashboards, and reduced the manual compliance workload dramatically. Also, user feedback affirmed that there were better understandings of roles, teamwork, and assurances of compliance processes. The research found that multi-framework compliance using the integrated Governance, Risk, and Compliance (GRC) capabilities of ServiceNow provided a scalable and effective solution in ensuring the continuity of adherence in the multi-frameworks to maintain proactive risk mitigation and adhere to regulatory resiliency in SaaS environments.

Keywords: *ServiceNow, SaaS Compliance, PCI-DSS, GDPR, SOX, Governance, Audit Automation, GRC Framework, Cloud Security, Regulatory Readiness.*

1. INTRODUCTION

The vigorous nature of cloud adoption and digital transformation initiatives has made the Software-as-a-Service (SaaS) platform the central core of the modern-day enterprise techno-space. Though SaaS platforms have the advantages of scalability, cost-efficiency and agility of operations, they also present the drawback of problematic governance and regulatory compliance challenges, particularly in highly-regulated industries, such as banking, healthcare and finance. The existing companies within the settings ought to ensure that they observe high standards of global regulations, including Payment Card Industry Data Security Standard (PCI-DSS), the General Data Protection Regulation (GDPR) and the Sarbanes-Oxley Act (SOX). The totality of these laws is to offer robust actions regarding information privateness, fiscal transparency, audit trail and risk control whereby there exists the necessity to have in place combined structures that are capable of constantly monitoring and implementing compliance needs.

The capability of the large workflow orchestration, the centralized audit administration and real-time monitoring capability should make ServiceNow a very significant enterprise platform in regard to governance, risk, and compliance (GRC) automation. Nevertheless, although it has a strong technological foundation, it still lacks a systematic academic and practice framework that proves how ServiceNow can be strategically used to operationalize compliance to various regulatory standards in SaaS settings. This paper has addressed that gap by gauging an automated controls, audit mechanisms, and ongoing compliance monitoring model with a ServiceNow focus that is intended to integrate across the areas of PCI, GDPR, and SOX.

One of the objectives of the research, through a mixed-method assessment, was to evaluate the efficacy of the model in the improvement of compliance maturity, audit preparedness, and transparency of the governance of the entire enterprise, which would add to the theoretical discussion and practical advice regarding SaaS regulatory management.

2. LITERATURE REVIEW

Rohatgi (2020) discussed the security issues in the context of cloud-based applications and highlighted the need to incorporate stringent security measures in SaaS designs as the only means to avoid data breaches and unauthorized access to information. Encryption, access controls, and unrelenting oversight of threats were mentioned as the best practices characterized by the study, and it was observed that those organizations that had organized security models had increased data protection and reliability in performing their operations within SaaS setups.

Mukherjee (2019) examined information governance issues related to adopting cloud computing and highlighted the necessity to establish the entire governance framework to guarantee the confidentiality of data, data integrity, and regulatory requirement. The results implied that those organizations that used cloud services without governance-alignment experienced compliance gaps, risk of mismanaged data, and operational wastefulness. The study emphasized policy development, data lifecycle, and compliance integration as some of the measures that are critical towards effective cloud governance.

Kaikkonen (2019) examined the problems of integrating SaaS applications and determined that interoperability problems, complexity of data synchronization, and absence of workflow consistency had impeded SaaS deployments. According to the reported study, compatibility of APIs, orchestration of services, and reliability of performance, when a combination of several SaaS platforms were involved, was a problem on the side of the enterprise, and thus, the standardization of automation and centralized management tools was necessary.

Novkovic and Korkut (2017) is dedicated to regulatory compliance in cloud settings and reported that cloud-based software and data systems needed to be followed in terms of following international regulatory frameworks. Their discussion made it clear that data exposure risks, failure to comply and audit failures were the results of inappropriate compliance management. The authors have confirmed that formal-compliance structures and computerized audit systems enhanced transparency and regulatory preparedness in the clouds.

Dzombeta (2016) established a change management compliance framework in cloud systems and proved that the cloud environments required dynamic compliance strategies as they constantly updated and changed configurations. The study hypothesized that the use of automated schemes of tracking change, enforcing policies, and the facility of audit trails were critical in ensuring a consistency of compliance to all the cloud services.

Ele and Oko (2016) studied the governance, risk, and compliance (GRC) systems, and concluded that integrated GRC models provided superior alignment of business goals, regulatory requirements, and IT activities. They reported in their analysis that companies that had integrated GRC systems attained better risk exposure, corporate discipline, and regulatory responsibility.

3. RESEARCH METHODOLOGY

3.1. Research Design

The study utilized a mixed approach to the research approach, qualitative and quantitative approaches. There were various organizational contexts analyzed using a multi-case study approach and compliance performance measured prior to and following the implementation of the ServiceNow-based governance model. The combination design methodology was applied to give a comprehensive evaluation of compliance maturity, system behavior and organizational outcomes.

3.2. Data Collection Methods

Primary Data

The IT compliance managers, ServiceNow architects, cybersecurity leaders and internal auditors participated in semi-structured interviews as primary data were collected. Employees in charge of compliance and audit activities were also surveyed to get an idea of how effective and ready they felt about the system. Furthermore, workflow automation was also observed directly, audit logs and policy-compliance dashboards in the ServiceNow environments were examined.

Secondary Data

The secondary sources consisted of regulatory documents, which were PCI DSS v4.0 guidelines, and GDPR articles, and SOX compliance frameworks. The research framework was supported by reviewing industry reports and audit findings, research on IT governance and SaaS compliance frameworks.

3.3. Study Sample and Selection

The study was carried out through purposive sampling on three organizations in the BFSI, healthcare, and IT services fields. The criteria of selection were on organizations that are actively deploying service now GRC features and those that need to comply with the compliance standards of PCI, GDPR, and/or SOX rules. Access to historical audit information and voluntary participation were also aspects that were considered during sample selection.

3.4. Tools and Platform

The research investigated governance and compliance processes that are enabled using the ServiceNow platform. Some of the modules that were examined were Policy and Compliance, Risk Management, Audit management and Security operations. The automation capacity of evidence collection, control mapping, compliance scoring and workflow orchestrating was evaluated specifically.

3.5. Data Analysis Techniques

The thematic analysis was applied to collected data to identify insights that can be obtained out of interviews and observations. Before and after the framework implementation, quantitative measures were statistically compared such as compliance readiness scores and duration of audit cycle. Control mapping matrix was designed to align ServiceNow controls with the requirements of PCI, GDPR and SOX to make an effective measurement of control.

3.6. Ethical Considerations

The study had ethical approval which was obtained prior to the commencement of the study. Anonymity was maintained on all organizational identities, audit records as well as internal compliance data. The participants gave informed consent, and all data were processed in the accordance with the ethical standards of research.

4. RESULTS AND DISCUSSION

This part gave the discoveries of the research and a critical interpretation of the results. The analysis of the data was performed to assess the usefulness of the ServiceNow-based governance and compliance model in enhancing regulatory preparedness in the field of PCI, GDPR, and SOX. The results indicated that compliance maturity, audit effectiveness, risk transparency, and controls execution automation significantly increased. These improvements have been found in the discussion to have an operational implication and how the abilities are consistent with enterprise regulatory requirements.

4.1. Improvement in Compliance Maturity Levels

As measured using the assistance of pre and post implementation reviews, compliance maturity scores had improved tremendously in all of the organizations that participated. The model that was introduced into ServiceNow improved the automated control testing, the monitoring of evidence and the regulation reporting.

Table 1: Compliance Maturity Score Comparison (Pre vs Post Implementation)

Organization	Compliance Frameworks (PCI/GDPR/SOX)	Pre-Implementation Score (1–5)	Post-Implementation Score (1–5)	Improvement (%)
Org A (BFSI)	PCI, SOX	2.8	4.3	+53.6%
Org B (Healthcare)	GDPR, PCI	3.1	4.5	+45.2%
Org C (IT Services)	SOX, GDPR	2.9	4.2	+44.8%

The high level of maturity indicated there existed a high degree of compliance gaps in the structured workflow of governance and automated evidence sources. The existence of the opportunity to map controls of ServiceNow to regulatory requirements increased the degree of traceability and accountability. These results were in line with the existing literature on the significance of technology-based compliance automation as a significant enabler of regulatory congruence.

4.2. Reduction in Audit Cycle Duration

The model reduced the hand work involved in collection of evidence and auditing preparation that resulted in speeding up of the audit period.

Table 2: Audit Cycle Duration (in working days)

Phase	Pre-Implementation	Post-Implementation	Reduction (%)
Audit Planning	10	6	40%
Evidence Collection	25	12	52%
Compliance Validation & Reporting	14	8	43%
Total Cycle Duration	**49 days**	**26 days**	**~47%** reduction

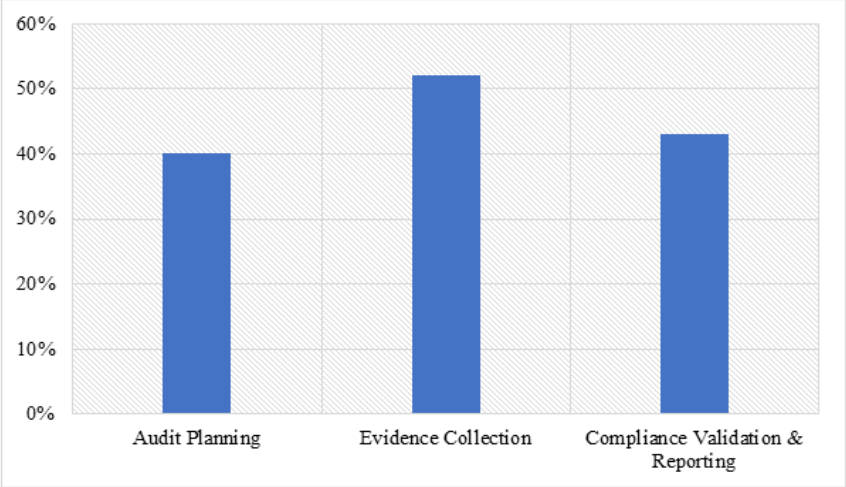

Figure 1: Audit Cycle Duration

The reduction in the audit time was justification of the advantages of the automatized workflow and the centralized audit repositories. The findings also showed that the structured audit trails and automated evidence connections at ServiceNow did not need redundancy anymore, and it improved the coordination between audit

and IT governance departments. This saving was worth the relevance of the integrated GRC platforms in the managed environment.

4.3. Enhanced Risk Visibility and Policy Governance

Automated alerts and real-time dashboards provided organizations with a better visibility of the risk. The workflows and policies on control were standardized and this reduced the interdepartmental inconsistencies.

Table 3: Risk and Policy Management Metrics

Evaluation Criteria	Pre-Implementation	Post-Implementation
Automated Risk Alerts	Low	High
Policy Version Tracking	Manual	Automated
Real-Time Compliance Dashboards	Not Available	Available
Centralized Evidence Repository	No	Yes
Cross-Departmental Compliance Collaboration	Limited	Strong

The enhancements meant that the integrated GRC modules of ServiceNow enabled sustained compliance checks and risk reduction. Regulatory deviation and weak policies enforcement structures were reduced through automated alerts and consistent policy enforcement structures. These results confirmed the perspective that continuous compliance systems are better than periodic manual checking especially in dynamic regulatory contexts.

4.4. Impact on Workforce Efficiency and Collaboration

Automation was associated with increased compliance responsibilities that were more clearly reported, less workload, and reduced compliance expenses incurred by the employees.

Table 4: User Feedback Summary

Feedback Criteria	Average Score (1–5)
Ease of workflow usage	4.2
Clarity of compliance responsibilities	4.4
Reduction in manual compliance tasks	4.0
Col3laboration between teams	4.3

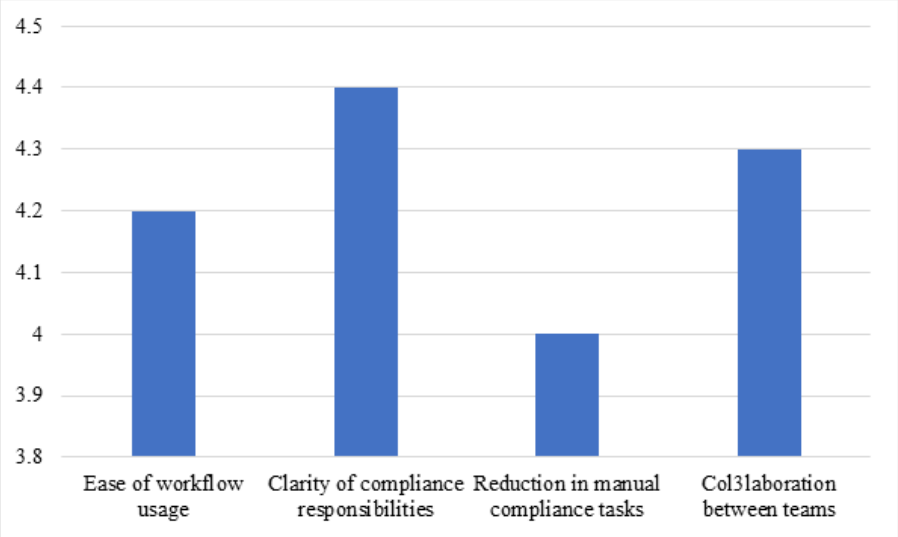

Figure 2: User Feedback Summary

The results were confirmed by the feedback of the quantitative gains through the metrics of operational performance. Not only the governance model enhanced the system-based compliance capabilities, but also the efficiency of the employees, transparency, and confidence in the procedures. With the compliance teams adapting to the automated workflow, the readiness of the organization to it on the technical and operational levels increased.

5. CONCLUSION

The results of this study revealed that a ServiceNow-focused model of governance and compliance can substantially enhance regulations SaaS preparedness in the framework of the PCI, GDPR, or SOX. This resulted in significant gains made by the implementation of automated control testing, centralized evidence repositories, policy governance workflows, and real-time compliance dashboards that resulted in significant improvements in compliance maturity, audit efficiency, and risk visibility. Almost 50 percent of the time savings in the audit cycles and significant increase in the level of governance maturity were registered in organizations, which substantiates the efficacy of automated governance operations in highly controlled sectors. In addition, greater interactions between compliance, risk and IT teams strengthened procedural conformity and responsibility. In general, the research validated that the combination of planned ServiceNow-based GRC practices offered a scalable, transparent, and future-oriented compliance model, making organizations poised to force ongoing regulatory compliance in the dynamic cloud ecosystems.

REFERENCES

1. *Aasi, P., Nikic, J., Li, M., & Rusu, L. (2020, November). The Influence of Cloud Computing on IT Governance in a Swedish Municipality. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 623-639). Cham: Springer International Publishing.*
2. *Dash, S., & Pani, S. K. (2016). E-Governance paradigm using cloud infrastructure: Benefits and challenges. Procedia Computer Science, 85, 843-855.*
3. *Dzombeta, S. (2016). Compliance framework for change management in cloud environments.*
4. *Ele, S. I., & Oko, J. O. (2016). Governance, risk and compliance (Grc): a. Journal of Integrative Humanism, 6(1), 161.*
5. *Hamid, H. A., Yusof, M. M., Dali, N. M., & Keroh, A. (2017). Security compliance behaviour of SaaS cloud users: A pilot study. Journal of Engineering and Applied Sciences, 12(16), 4150-4155.*
6. *Hashmi, A., Ranjan, A., & Anand, A. (2018). Security and compliance management in cloud computing. International Journal of Advanced Studies in Computers, Science and Engineering, 7(1), 47-54.*
7. *Kaikkonen, T. (2019). SaaS application integration challenges.*
8. *Khalil, S., Fernandez, V., & Fautrero, V. (2016, August). Cloud impact on IT governance. In 2016 IEEE 18th conference on business informatics (CBI) (Vol. 1, pp. 255-261). IEEE.*
9. *Mukherjee, S. (2019). Information governance for the implementation of cloud computing. Available at SSRN 3405102.*
10. *Novkovic, G., & Korkut, T. (2017). Software and Data Regulatory Compliance in the Cloud. Software quality professional, 20(1).*
11. *Owuonda, S. O. (2016). Cloud Computing Governance Readiness Assessment: Case Study of a local Airline Company (Doctoral dissertation, University of Nairobi).*
12. *Rohatgi, G. (2020). Ensuring Secure SaaS: Best Practices and Approaches for Integrating Security to Cloud-Based Applications. Journal of Technological Innovations, 1(2), 8-8.*

13. *Singh, A. (2020). A Framework for a Standard Compliance Architecture (Doctoral dissertation, Pace University).*

14. *Walko, J., Olney, M., & Hunt, D. (2020). The rise of SaaS ERP solutions. Management in Healthcare, 4(4), 340-349.*

15. *Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. Journal of Internet Services and Applications, 7(1), 5.*