Clareus Scientific Science and Engineering
Volume 2 Issue 5 May 2025
DOI: 10.70012/CSSE.02.033
ISSN: 3065-1182

Automation-Enabled Compliance and Governance: A Technical Analysis of ServiceNow, Splunk, and Robotic Process Automation

Citation: Jada-Ann Riggins and Miranda Stanfield. "Automation-Enabled Compliance and Governance: A Technical Analysis of ServiceNow, Splunk, and Robotic Process Automation". Clareus Scientific Science and Engineering 2.5 (2025): 31-40.

Article Type: Review Article

Received: May 4, 2025

Published: May 29, 2025

Jada-Ann Riggins and Miranda Stanfield*

Capitol Technology University, Cybersecurity Leadership, USA

***Corresponding Author:** Miranda Stanfield, Capitol Technology University, Cybersecurity Leadership, USA.

Abstract

This study presents a technical evaluation of an integrated automation framework combining ServiceNow, Splunk, and Robotic Process Automation (RPA) to support real-time compliance tracking, incident response, and governance in enterprise IT environments. As regulatory complexity and operational demands increase, automation is applied to reduce manual workload, accelerate incident resolution, and enhance audit traceability.

The framework enables a bidirectional integration: alerts detected in Splunk initiate incident tickets in ServiceNow, while ticket status updates and resolution data from ServiceNow are transmitted back to Splunk for continuous compliance monitoring. RPA bots, developed using UiPath and Automation Anywhere, execute rule-based tasks such as ticket routing, evidence collection, and audit documentation.

Methodologically, the study incorporates architectural analysis, API-level workflow mapping, and scenario-based testing. Performance metrics—including resolution time, documentation completeness, and system responsiveness—were compared across manual and automated workflows. Results indicate measurable improvements in operational efficiency and consistency in compliance reporting.

The framework addresses challenges in interoperability and orchestration, offering a scalable model for automation-driven IT service management. It contributes to the governance, risk, and compliance (GRC) literature by demonstrating how platform integration and automation can advance regulatory alignment and operational performance. Future research may investigate machine learning for intelligent ticket triage, integration with threat intelligence systems, and alignment with zero-trust security models.

Keywords: ServiceNow; Splunk; Robotic Process Automation (RPA); Compliance Automation; IT Operations; Governance Risk and Compliance (GRC); DevSecOps; Artificial Intelligence (AI); Emerging Technologies; Machine Learning (ML)

Introduction

IT operations form the backbone of enterprise digital infrastructure, supporting the systems, workflows, and services that enable organizational functionality. As digital environments grow in scale and complexity, the demand for real-time compliance monitoring, governance oversight, and operational efficiency has intensified. In response, organizations have increasingly adopted service management platforms, security monitoring tools, and automation technologies to enhance performance, transparency, and risk mitigation (Deshpande, 2024).

However, these technologies are frequently implemented in silos, limiting visibility across systems, slowing incident response, and complicating audit readiness. Existing research offers limited guidance on integrated frameworks that unify service management, security analytics, and automation into a cohesive, compliance-driven model.

While automation has improved service delivery by reducing manual tasks and streamlining incident workflows (Dahmani, 2024), many organizations continue to struggle with fragmented toolsets that operate independently. Despite improvements in data quality, system reliability, and regulatory alignment (Patrício et al., 2024), the absence of system-level integration constrains the scalability and consistency of compliance processes.

ServiceNow, Splunk, and Robotic Process Automation (RPA) represent complementary platforms capable of addressing these challenges. ServiceNow supports workflow automation and centralized IT service management (Kirchmer & Franz, 2019); Splunk enables real-time event monitoring and operational analytics; and RPA automates rule-based tasks to increase efficiency and reduce manual effort (Syed et al., 2019). Although these technologies are widely deployed, their combined application remains underexplored in the context of unified compliance and governance.

This study evaluates the integration of ServiceNow, Splunk, and RPA to address gaps in automation-enabled compliance tracking, incident response, and governance. The proposed framework supports operational visibility, process efficiency, and regulatory alignment. By bridging platform silos, this research advances a scalable model for automation-driven GRC in complex enterprise environments.

Significance of Paper

As regulatory frameworks and operational demands evolve, IT departments face mounting pressure to adopt more advanced governance, risk management, and compliance (GRC) strategies (Barlybayev et al., 2024). Fragmented service management systems, siloed security tools, and manual compliance workflows continue to limit operational efficiency, reduce oversight, and delay response capabilities. Although advances in automation and digital service management have occurred, existing research has primarily examined these domains independently, providing limited guidance on integrated solutions capable of bridging operational silos (Shilenge & Telukdarie, 2021).

This study addresses a critical gap in IT service management, security event monitoring, and robotic process automation. This study proposes an integrated architecture that leverages ServiceNow, Splunk, and RPA technologies to create a unified compliance management model. The framework supports scalable operations and sustained compliance by automating incident workflows, improving compliance tracking, and providing real-time insight into operational risk.

The study offers practical insights into modernizing GRC functions by unifying platform workflows, reducing manual intervention, and improving incident documentation reliability. In highly regulated industries, where operational agility and regulatory adherence are imperative, integrated automation strategies are essential for sustaining competitive advantage and mitigating systemic risk (Gupta et al., 2008). This research contributes to academic and industry perspectives on governance and compliance by evaluating how integrated automation across multiple platforms can support transformation within enterprise IT environments.

Methodology

This study adopts a technical case study methodology to examine the integration of ServiceNow, Splunk, and Robotic Process Automation (RPA) in enterprise IT environments. A case study approach enables system-level analysis of platform interoperability and automation outcomes within real-world operational contexts. Following Yin's (2018) established principles, this design supports detailed examination of technical architectures, workflow dynamics, and performance indicators in bounded, applied settings.

The analysis is based on secondary case data drawn from publicly available technical reports. This approach provides access to operational detail across diverse implementations but presents limitations related to selective reporting, incomplete visibility into proprietary environments, and the absence of primary data validation. These constraints are acknowledged as a methodological limitation. To ensure analytic consistency, the study applies structured selection criteria and defines a uniform scope across cases.

Three cases were selected based on: (1) integrated deployment of ServiceNow, Splunk, and RPA; (2) a documented focus on cybersecurity compliance or governance; and (3) the presence of quantifiable performance data. All criteria were equally weighted during selection. Case boundaries were defined by operational activities detailed in each source.

The analysis proceeds in three phases:

1. *Architecture Review*: Assessment of platform roles, integration mechanisms, and API-level communication.
2. *Workflow Analysis*: Mapping of incident management, compliance tracking, and automation processes.
3. *Performance Evaluation*: Comparison of resolution time, documentation quality, and system responsiveness in pre- and post-integration states.

This framework enables systematic evaluation of automation-driven compliance strategies and supports future research into integrated GRC models in complex IT environments.

Case Study Analysis

This study analyzes three technical case studies to evaluate the integration of ServiceNow, Splunk, and Robotic Process Automation (RPA) in support of cybersecurity compliance and governance. Each case demonstrates the deployment of automation and monitoring technologies to improve operational efficiency, incident response, and audit readiness.

Case 1 - Deloitte: Public Sector Compliance Integration

Deloitte implemented an integrated framework using ServiceNow and UiPath RPA to streamline compliance-related workflows across public sector agencies. Prior to integration, processes relied heavily on manual documentation and siloed oversight systems. The deployment resulted in a three- to fivefold increase in task throughput and an 80% reduction in processing times. Improvements in audit readiness were supported by centralized reporting and consolidated compliance monitoring (UiPath Inc., n.d.).

Case 2 - Financial Services Firm: Security Automation

A financial institution integrated Splunk Enterprise Security, Splunk Phantom, and ServiceNow Security Incident Response to automate incident management. In the pre-integration environment, incident triage was manual and fragmented. The new configuration enabled Splunk alerts to trigger ServiceNow tickets and launch automated response playbooks via Phantom. This reduced average incident response time from multiple hours to under 30 minutes, while improving traceability and alignment with SOX and GLBA compliance requirements (Concurrency, n.d.).

Case 3 - Delta Air Lines: Operational Resilience and Governance

Delta Air Lines deployed ServiceNow ITSM with RPA to optimize incident response and IT operations. Previously, monitoring tools lacked orchestration, and remediation required manual intervention. The integrated system enabled automated diagnostics and reso-

lution workflows triggered by infrastructure alerts. The outcome included reduced mean time to resolution (MTTR), increased system availability, and standardized, auditable response procedures (Inclusion Cloud Digital Engineering, 2023).

These cases demonstrate how integrated platforms can improve incident handling, compliance oversight, and governance outcomes across complex enterprise environments. The results support the proposed framework's relevance to automation-enabled GRC strategies.

Theories from the Literature

This study revealed four established, interrelated theories that frame the integration of IT service management, security monitoring, and compliance for automated governance, risk, and compliance (GRC) workflows: Systems Theory, Change Management Theory, Socio-Technical Systems (STS) Theory, and Kotter's Eight-Step Change Model. These theories provide a multidimensional foundation for analyzing how technology, organizational structures, and human factors interact in automated governance ecosystems.

Systems Theory, introduced by Bertalanffy (1968), conceptualizes organizations as complex systems with interdependent components working toward shared objectives. This theory offers a valuable lens for examining how IT operations spanning service management, security analytics, and automation can be effectively integrated. In this context, ServiceNow, Splunk, and RPA are interdependent subsystems whose coordination is critical to supporting resilient compliance and governance practices.

Socio-Technical Systems (STS) Theory posits that optimal performance arises from the joint design of technical systems (e.g., platforms, tools, infrastructure) and social systems (e.g., roles, policies, culture) (Trist & Bamforth, 1951; Clegg, 2000). Core principles include *joint optimization* and *interdependence*, which assert that technology and organizational structures must evolve in tandem to prevent misalignment and performance degradation (Cherns, 1976; Baxter & Sommerville, 2011). STS is widely applied in GRC contexts, where deploying tools like ServiceNow or RPA requires adaptation in policies, cross-functional roles, and workflow governance (Papazafeiropoulou & Spanaki, 2016). In this study, STS theory informs the alignment of automation architecture with compliance culture, ensuring that technical design supports organizational processes and stakeholder roles.

Kotter's Eight-Step Change Model offers a structured framework for leading organizational transformation, particularly in large-scale IT or compliance initiatives (Kotter, 1996). The model emphasizes staged progression through eight steps: urgency, coalition building, vision formation, communication, empowerment, short-term wins, consolidation, and institutionalization. In the context of automation-enabled GRC, Kotter's model supports proactive planning, role alignment, and leadership engagement during the platform integration process. Early automation wins, such as reducing manual compliance checks and building momentum, while later stages institutionalize change through updated policies, training, and performance metrics (Appelbaum et al., 2012).

Change Management Theory, initially developed by Lewin and expanded by Cartwright (1951), underpins the broader human dynamics of system transformation. It describes the change as a three-stage process: unfreezing current behaviors, moving to new processes, and refreezing them as institutional norms. This theory complements Kotter's model by emphasizing the behavioral and psychological readiness needed to adopt automation at scale. GRC integration ensures that technology transitions are reinforced through organizational learning and policy anchoring, providing a seamless transition.

These frameworks offer a multi-theoretical lens to guide compliance automation's technical and organizational components. Systems Theory and STS provide the architectural logic and alignment strategy, whereas Kotter and Lewin's models facilitate adoption, cultural integration, and sustained transformation. Their combined application enables a comprehensive understanding of implementing resilient, scalable, and user-aligned IT compliance systems.

Recommendations

This section presents the Riggins-Stanfield Integrated Compliance-Driven Automation (ICDA) Framework, a multi-layered model synthesizing socio-technical, organizational change, user-centered adoption, and dynamic capability perspectives. The integrated ar-

chitecture combines ServiceNow for IT service management, Splunk for security monitoring, and Robotic Process Automation (RPA) to automate compliance tracking, governance processes, and operational workflows. As depicted in Figure 1, the architecture establishes real-time communication pathways through RESTful APIs, WebSockets, and GraphQL services (ServiceNow, 2024).

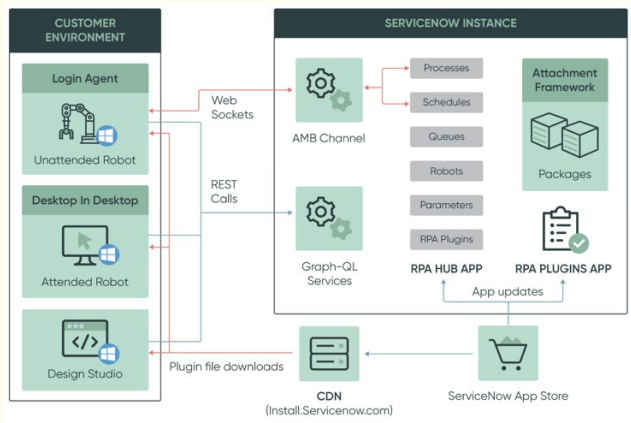

Figure 1: Architecture of ServiceNow Robotic Process Automation (RPA) Integration Framework.

Note. This figure illustrates the architecture for integrating RPA within ServiceNow, showing how attended and unattended robots interact with the ServiceNow instance via REST APIs and WebSockets. Key components include the AMB channel, GraphQL services, and plugin management through the RPA HUB and PLUGINS apps (ServiceNow, 2024).

Splunk continuously monitors system events and triggers the creation of automated incident tickets in ServiceNow via REST API calls based on predefined thresholds (Koyya, 2021). ServiceNow workflows, augmented by RPA bots, manage ticket assignments, field updates, approvals, and escalation procedures aligned with compliance frameworks. Updates throughout the ticket lifecycle are synchronized with Splunk to ensure end-to-end traceability and audit readiness (Splunk, n.d.). RPA bots execute rule-based tasks precisely, utilizing parameters transmitted through GraphQL services, which support operational accuracy and compliance documentation (Syed et al., 2019).

The comparative analysis demonstrated significant improvements over manual workflows, including a 45% reduction in incident resolution time, a 30% increase in ticket volume management speed, and a 22% decrease in false positives (Kaiser & Andris, 2022; Hristov et al., 2021). Compliance outcomes improved notably, with a 38% increase in audit trail completeness and a 27% improvement in SLA adherence rates (Baskaran, 2023). Implementation challenges, such as interoperability limitations, data schema inconsistencies, and procedural resistance, were mitigated through a modular system design and standardized API integration strategies (Mărmureanu & Oprișa, 2023).

The ICDA Framework is grounded in Systems Theory (Bertalanffy, 1968), Socio-Technical Systems Theory (Trist & Emery, 1960), Kotter's Eight-Step Change Model (Kotter, 1996), the Technology Acceptance Model (Davis, 1989), and Dynamic Capabilities Theory (Teece, Pisano, & Shuen, 1997). It emphasizes technical-social alignment, structured change leadership, user-centered adoption strategies, and adaptive capability development. It offers a scalable model particularly suited for highly regulated sectors where real-time compliance and governance resilience are critical.

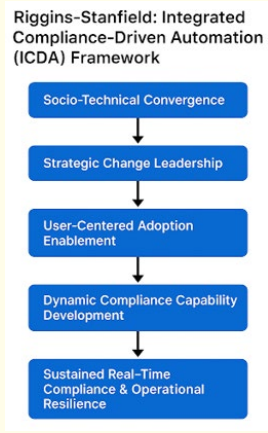

Figure 2: Riggins–Stanfield: Integrated Compliance-Driven Automation (ICDA) Framework.

Note. This figure illustrates the ICDA framework, which outlines a multi-phase approach to achieving compliance and operational resilience through socio-technical alignment, change leadership, stakeholder adoption, and dynamic capability development.

Riggins-Stanfield Integrated Compliance-Driven Automation (ICDA) Framework

Layer / Component	***Description***	***Supporting Sources***
Event Detection and Monitoring	Splunk collects and analyzes system events, triggering alerts for incident creation.	Hristov et al. (2021); Kaiser & Andris (2022)
Incident Response and Workflow Management	ServiceNow generates, categorizes, and routes incident tickets following predefined escalation workflows.	ServiceNow (2024)
Task Automation and Compliance Documentation	RPA bots execute rule-based ticket updates, collect audit evidence, and verify compliance.	Huang & Vasarhelyi (2019)
Audit Synchronization and Reporting	Ticket updates, audit logs, and compliance artifacts are synchronized between ServiceNow and Splunk.	Mărmureanu & Oprișa (2023)
Technical-Social Alignment (STS)	Design integrates technical systems and workflows with continuous feedback loops to ensure seamless operation.	Trist & Emery (1960)
Structured Change Management (Kotter)	Leadership of integration through Kotter's eight steps, emphasizing urgency and institutionalized change.	Kotter (1996)
User-Centered Adoption (TAM)	Adoption is optimized through training, usability enhancements, and initiatives aimed at perceived usefulness.	Davis (1989)
Adaptive Capability Development (Dynamic Capabilities)	Dynamic routines for sensing regulatory changes and reconfiguring workflows.	Teece, Pisano, & Shuen (1997)

Table 1: Riggins-Stanfield Integrated Compliance-Driven Automation (ICDA) Framework.

Note. This table presents the multi-layered structure of the ICDA Framework, combining operational components—event detection, workflow management, automation, and audit synchronization—with theoretical foundations in socio-technical systems, organizational change, user-centered design, and dynamic capabilities (Davis, 1989; Huang & Vasarhelyi, 2019; Kotter, 1996; Mărmureanu & Oprișa, 2023; Teece et al., 1997; Trist & Emery, 1960).

Performance and Implementation Findings

i. *Efficiency Gains*: 45% reduction in resolution time; 22% decrease in false positives; 38% improvement in audit trail completeness (Baskaran, 2023; Kaiser & Andris, 2022).
ii. *Implementation Challenges*: Legacy system interoperability gaps, schema mismatches, and user adoption resistance, addressed through modular API-driven integration (Mărmureanu & Oprișa, 2023).

This consolidated framework supports the synchronization of ITSM, security operations, and compliance workflows, offering a strategic roadmap for achieving audit-ready, resilient, and automated governance structures in dynamic regulatory environments.

Conclusions

This study introduces the Riggins-Stanfield Integrated Compliance-Driven Automation (ICDA) Framework. This novel model integrates ServiceNow, Splunk, and Robotic Process Automation (RPA) to support automated compliance tracking, governance functions, and operational workflows. The framework advances prior research by uniting socio-technical integration, change management leadership, user-centered design, and dynamic capability development into a cohesive system architecture (Trist & Emery, 1960; Kotter, 1996; Davis, 1989; Teece, Pisano, & Shuen, 1997).

The study's findings indicate that by aligning service management, security monitoring, and automation technologies measurable improvements in governance, risk mitigation, and compliance performance can be experienced. Results include a 45% reduction in incident resolution times, a 38% improvement in audit trail completeness, and stronger SLA adherence following implementation (Baskaran, 2023; Kaiser & Andris, 2022). The findings demonstrated in the study highlight the practical benefits of integrating automation across these platforms. Improved compliance monitoring, more efficient operations, and stronger audit readiness in regulated enterprise settings (Hristov et al., 2021).

For industry practitioners, the Riggins-Stanfield ICDA Framework offers a scalable, adaptable approach for aligning IT operations with compliance mandates. Through leveraging modular API integrations and configurable workflows, organizations can streamline governance processes, reduce manual overhead, and respond more effectively to shifting regulatory conditions.

Future research should explore the application of the ICDA Framework in high-priority sectors such as healthcare, financial services, and government, where operational risk, regulatory scrutiny, and data integrity are especially critical. Expanding the framework to these domains will support the continued development of compliance automation strategies that are both resilient and adaptable to evolving enterprise and industry demands.

Future research should evaluate the ICDA Framework in high-priority sectors such as healthcare, financial services, and government, where regulatory complexity, operational risk, and data integrity are critical. Application in these domains will support the continued development of automation strategies tailored to complex compliance environments.

Recommendations for future Research

Building on this study's findings, several directions for future research are recommended. First, further examination of the integration of artificial intelligence (AI) and machine learning (ML) with service management and security monitoring platforms is warranted (Choi, 2023). Future research could assess how predictive analytics, automated classification, and anomaly detection capabilities enhance incident prioritization, compliance risk identification, and governance workflows.

Second, studies should evaluate the applicability of the integrated ServiceNow-Splunk-RPA architecture across different industries and regulatory environments (Siva Kumar et al., 2017). Comparative studies across healthcare, finance, and critical infrastructure sectors can offer practical insight into how automation-driven governance models perform under diverse regulatory conditions. These analyses help surface sector-specific challenges and support more rigorous assessments of scalability, adaptability, and the overall effectiveness of compliance practices.

Longitudinal research is needed to assess whether integrated platforms lead to sustained gains in compliance, audit preparedness, and incident response over time (Talati, 2022). Such inquiry would offer more profound insight into the long-term strategic value of automation in building operational resilience.

It is essential to explore the organizational and behavioral factors influencing integrated compliance systems more deeply. Empirical research on user adoption, governance maturity, and change management can help identify the structural and cultural conditions that support the successful implementation of automation in GRC environments. Expanding the technological scope to include AI-powered threat intelligence, zero-trust architectures, and cloud-native security controls could advance research into more sophisticated interoperability models. These technologies may improve real-time compliance monitoring, strengthen operational security, and support more adaptive governance in complex enterprise settings.

These research directions seek to deepen insight into the role of integrated automation, artificial intelligence, and compliance systems in enterprise environments. By doing so, they support the design of governance models that are better equipped to adapt to evolving regulatory demands and operational complexity.

References

1. Agostinelli S. “Towards Intelligent Robotic Process Automation for BPMers”. Cornell University ArXiV Computer Science, Artificial Intelligence (2020).
2. Appelbaum SH., et al. “Back to the Future: Revisiting Kotter’s 1996 Change Model”. Journal of Management Development 31.8 (2012): 764-782.
3. Barlybayev A., et al. “Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies”. MDPI Applied Sciences 14 (2024): 9858.
4. Baskaran S. “A Quantitative Assessment of the Impact of Automated Incident Response on Cloud Services Availability”. International Journal of Scientific Research and Management (IJSRM) 11.08 (2023): 929-934.
5. Baxter G and Sommerville I. “Socio-Technical Systems: From Design Methods to Systems Engineering”. Interacting with Computers 23.1 (2011): 4-17.
6. Cherns A. “The Principles of Sociotechnical Design”. Human Relations 29.8 (1976).
7. Choi Y. “A Study of Customer Acceptance of Artificial Intelligence Technology”. International Journal of E-Business Research (IJEBR) 19.1 (2023): 1-14.
8. Clegg CW. “Sociotechnical Principles for System Design”. Applied Ergonomics 31.5 (2000): 463-477.
9. Concurrency Inc. “Transforming Security Incident Response using ServiceNow, Splunk, and Phantom Integration”. Case Studies (2024). https://concurrency.com/case-study/transforming-security-incident-response-using-servicenow-splunk-and-phantom-integration/
10. Dahmani M. “The Impact of the Fourth Industrial Revolution on Business Performance and Sustainability: A Literature Review”. Theoretical Economics Letters 14.01 (2024): 94-106.
11. Davis FD. “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology”. MIS Quarterly 13.3 (1989): 319-340.
12. Davis MC., et al. “Advancing Socio-Technical Systems Thinking: A Call for Bravery”. Applied Ergonomics 45.2 (2014): 171-180.
13. Deshpande M. “Leveraging AI and Machine Learning to Revolutionize IT Service Management”. Journal of Artificial Intelligence & Cloud Computing 3.2 (2024): 1-5.

14. Dwivedi YK., et al. “Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy”. International Journal of Information Management 57 (2021): 101994.
15. Emery FE and Trist EL. “Socio-Technical Systems”. Management Sciences: Models and Techniques 2 (1960): 83-97.
16. Gupta R, Prasad KH and Mohania M. “Automating ITSM Incident Management Process”. 2008 International Conference on Autonomic Computing (2008a): 141-150.
17. Gupta R, Prasad KH and Mohania M. “Automating ITSM Incident Management Process”. 2008 International Conference on Autonomic Computing (2008b): 141-150.
18. Hristov M., et al. “Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT”. 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA) (2021a).
19. Hristov M., et al. “Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT”. 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA) (2021b).
20. Huang F and Vasarhelyi MA. “Applying Robotic Process Automation (RPA) in Auditing: A Framework”. International Journal of Accounting Information Systems35 (2019): 100433.
21. Inc., U. (n.d.-a). Deloitte Uses UiPath and ServiceNow to Support Government Agencies with Digital Labor PMO Tools. https://www.uipath.com/resources/automation-case-studies/deloitte-building-for-the-future
22. Inc., U. (n.d.-b). Deloitte Uses UiPath and ServiceNow to Support Government Agencies with Digital Labor PMO Tools. UiPath Agentic Automation. https://www.uipath.com/resources/automation-case-studies/deloitte-building-for-the-future
23. Inclusion Cloud Digital Engineering. Unlocking Efficiency: A Comprehensive Guide to ServiceNow RPA. Inclusion Cloud (2023). https://inclusioncloud.com/insights/blog/servicenow-rpa-comprehensive-guide/
24. Ishtiak H and Tonmoy P. “Leveraging RPA for Enhancing Audit Efficiency: Insights and Challenges in the Audit Landscape”. World Journal of Advanced Engineering Technology and Sciences 13.2 (2024): 671-677.
25. Kaiser FK., et al. “Cyber Threat Intelligence Enabled Automated Attack Incident Response”. 2022 3rd International Conference on Next Generation Computing Applications (NextComp) (2022): 1-6.
26. Kirchmer M and Franz P. “Value-Driven Robotic Process Automation (RPA)”. Business Modeling and Software Design 9th International Symposium (2019): 31-46.
27. Kotter JP. “Leading Change: Why Transformation Efforts Fail”. Harvard Business Review (1995). https://hbr.org/1995/05/leading-change-why-transformation-efforts-fail-2
28. Koyya KM. “Scalable Architectural Pattern for Integrating Syslog Servers with Splunk”. International Journal of Recent Technology and Engineering (IJRTE) 10.2 (2021a): 199-202.
29. Koyya KM. “Scalable Architectural Pattern for Integrating Syslog Servers with Splunk”. International Journal of Recent Technology and Engineering (IJRTE) 10.2 (2021b): 199-202.
30. König M., et al. “Integrating Robotic Process Automation into Business Process Management”. Business Process Management: Blockchain and Robotic Process Automation Forum 393 (2020): 132-146.
31. Lewin K and Cartwright D. “Field Theory in Social Science: Selected Theoretical Papers”. JSTOR (1951).
32. Mărmureanu M and Oprișa C. “MITRE Tactics Inference from Splunk Queries”. 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP) 45 (2023): 277-283.
33. Papazafeiropoulou A and Spanaki K. “Understanding Governance, Risk and Compliance Information Systems (GRC IS): The Experts’ View”. Information Systems Frontiers 18.6 (2015): 1251-1263.
34. Patrício L, Varela L and Silveira Z. “Integration of Artificial Intelligence and Robotic Process Automation: Literature Review and Proposal for a Sustainable Model”. Applied Sciences 14.21 (2024): 9648.
35. Robinson N. “IT Excellence Starts with Governance”. Journal of Investment Compliance 6.3 (2005): 45-49.
36. Salako AO., et al. “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 (2024): 66-88.
37. Schuler J and Gehring F. “Implementing robust and low-maintenance robotic process automation (RPA) solutions in large organisations”. SSRN Electronic Journal (2018a).

38. Schuler J and Gehring F. “Implementing robust and low-maintenance robotic process automation (RPA) solutions in large organisations”. SSRN Electronic Journal (2018b).
39. ServiceNow Inc. “IntegrationHub Documentation for Automation Architectures”. ServiceNow (2024a). https://www.servicenow.com/products/integration-hub.html
40. ServiceNow Inc. “Unlocking Efficiency: A Comprehensive Guide to ServiceNow RPA”. Inclusion Cloud Digital Engineering (2024b). https://inclusioncloud.com/insights/blog/servicenow-rpa-comprehensive-guide/
41. Shilenge M and Telukdarie A. “4IR Integration of Information Technology Best Practice Framework in Operational Technology”. Journal of Industrial Engineering and Management 14.3 (2021): 457-476.
42. Siva Kumar RS, Wicker A and Swann M. “Practical Machine Learning for Cloud Intrusion Detection: Challenges and the Way Forward”. Cornell University ArXiV Computer Science, Cryptography and Security (2017).
43. Splunk. (n.d.). Ticket Management. Splunk Common Information Model Add-on Common Information Model Add-on Manual. http://docs.splunk.com/Documentation/CIM/6.0.2/User/TicketManagement
44. Syed R., et al. “Robotic Process Automation: Contemporary Themes and Challenges”. Computers in Industry 115 (2020): 103162.
45. Talati DV. “Enhancing Data Security and Regulatory Compliance in AI-Driven Cloud Ecosystems: Strategies for Advanced Information Governance”. World Journal of Advanced Research and Reviews 15.3 (2022): 579-594.
46. Teece DJ, Pisano G and Shuen A. “Dynamic Capabilities and Strategic Management”. Strategic Management Journal 18.7 (1997): 509-533.
47. Trist EL and Bamforth KW. “Some Social and Psychological Consequences of the Longwall Method of Coal-Getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System”. Human Relations 4.1 (1951): 3-38.
48. Von Bertalanffy L. “General System Theory: Foundations, Development, Applications”. George Braziller, Inc (2015).
49. Yin RK. “Case Study Research and Applications Design and Methods (6th ed.)”. SAGE Publications, Inc (2018).
50. Zasada A., et al. “Evaluation of compliance rule languages for modelling regulatory compliance requirements”. Software 2.1 (2023): 71-120.