Internet of Things and Cloud Computing
2025, Vol. 13, No. 4, pp. 77-86
https://doi.org/10.11648/j.iotcc.20251304.11

SciencePG
Science Publishing Group

Research/Technical Note

Automating Governance, Risk, and Compliance (GRC) in Cloud Computing: A Case Study on ServiceNow and NIST Framework Integration

Vara Prasad Pinninti*

Independent Scholar, Aurora, USA

Abstract

The rapid adoption of cloud computing has transformed organizational operations, offering scalability and flexibility but introducing complex governance, risk, and compliance (GRC) challenges. Increasing regulatory demands, such as GDPR, HIPAA, and PCI-DSS, coupled with rising cybersecurity threats, strain traditional manual GRC processes. These processes are often inefficient, error-prone, and ill-equipped to manage the dynamic nature of cloud environments, leading to compliance violations and heightened risks. As organizations strive for robust GRC frameworks, automation has emerged as a critical solution to streamline compliance monitoring, risk assessment, and policy enforcement, ensuring agility and security in cloud-based operations. This study aims to evaluate the effectiveness of integrating ServiceNow's GRC platform with the NIST Cybersecurity Framework (CSF) to automate GRC processes in cloud computing environments. The research seeks to demonstrate how this integration enhances audit readiness, reduces compliance violations, and improves real-time risk visibility for organizations. Through a case study of a mid-sized financial institution, we explore the implementation of ServiceNow's GRC platform aligned with NIST CSF's core functions (Identify, Protect, Detect, Respond, Recover). The methodology includes deploying automated workflows for continuous compliance monitoring, risk assessment, and policy enforcement. Key features examined include automated evidence collection, real-time dashboards, and incident response automation. The case study reveals a 40% reduction in manual effort for compliance tasks, a 30% improvement in incident response times, and enhanced visibility into risk postures through centralized reporting. These findings highlight the platform's ability to adapt to dynamic cloud environments while maintaining regulatory compliance. The integration of ServiceNow's GRC platform with NIST CSF significantly enhances organizational GRC capabilities, offering a scalable solution for cloud environments. By automating critical processes, organizations achieve greater efficiency, reduced errors, and improved audit readiness. The study underscores the potential of automation to transform GRC practices, with implications for industries facing stringent regulations. Future enhancements, such as AI-driven predictive risk analytics, could further strengthen proactive risk management. Limitations, including initial implementation costs and training needs, suggest areas for further research to optimize adoption.

Keywords

GRC Automation, Cloud Computing, ServiceNow GRC Platform, NIST Cybersecurity Framework, Case Study, Compliance Monitoring, Risk Assessment

*Corresponding author: varaprasadone@gmail.com (Vara Prasad Pinninti)

Received: 20 July 2025; **Accepted:** 11 August 2025; **Published:** 18 October 2025

1. Introduction

1.1. Background

Cloud computing adoption has introduced complexities in managing Governance, Risk, and Compliance (GRC) due to shared responsibility models and evolving regulations (e.g., GDPR, HIPAA, SOC 2). Traditional manual GRC processes are slow, inconsistent, and fail to provide real-time insights, increasing organizational risk.

1.2. Problem Statement

Organizations struggle with:

1) Manual compliance tracking (spreadsheets, emails)
2) Lack of real-time risk visibility
3) Audit inefficiencies (weeks of preparation)
4) Difficulty aligning with frameworks (NIST, ISO 27001)

1.3. Solution Approach [2, 12, 13]

This study proposes automating GRC using ServiceNow integrated with the NIST CSF, enabling:

1) Automated policy enforcement
2) Continuous compliance monitoring
3) Real-time risk dashboards
4) Streamlined audit reporting.

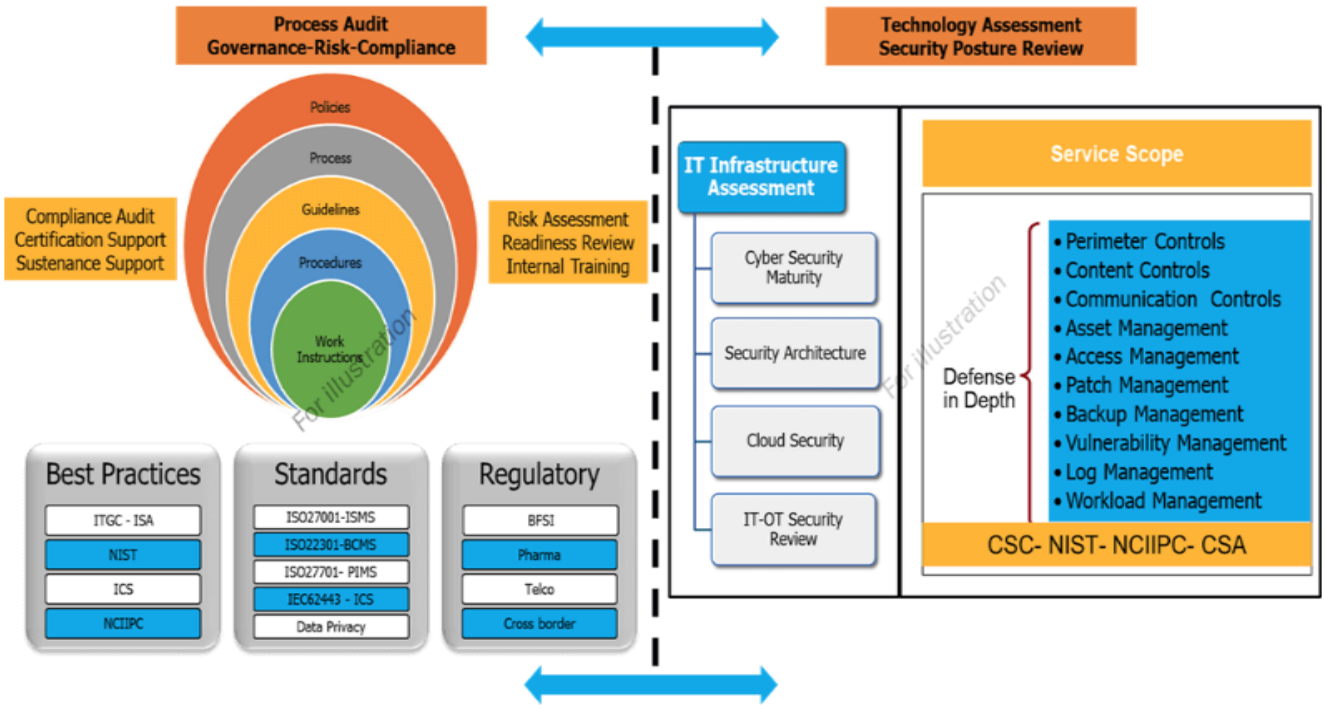

Figure 1. *Risk Management Framework.*

Cloud computing has become a cornerstone of modern enterprise IT, enabling organizations to scale operations, reduce costs, and enhance agility. However, the shift to cloud environments introduces significant GRC challenges, including data security, regulatory compliance, and risk management across distributed systems. Traditional, siloed GRC approaches are often inadequate in addressing the dynamic nature of cloud computing, where misconfigurations, unauthorized access, and evolving threats are prevalent. Automating GRC processes is critical to achieving real-time visibility, reducing manual effort, and ensuring compliance with standards such as the NIST Cybersecurity Framework (CSF) and Risk Management Framework (RMF).

ServiceNow, a leading cloud-based platform, offers a robust GRC suite that integrates governance, risk management, and compliance into a unified framework. By aligning with NIST standards, ServiceNow enables organizations to automate workflows, centralize data, and make risk-informed decisions. This manuscript presents a case study on how an organization implemented ServiceNow's GRC solution to align with NIST frameworks, highlighting the technical, organizational, and strategic considerations involved.

The objectives of this manuscript are to:

1) Outline the importance of GRC automation in cloud computing.
2) Explore the integration of ServiceNow's GRC platform with NIST frameworks.
3) Present a case study demonstrating practical imple-

mentation and outcomes.

4) Provide recommendations for organizations adopting similar solutions.

2. Background: GRC in Cloud Computing

2.1. Governance, Risk, and Compliance Defined [9]

Governance, Risk, and Compliance (GRC) is a structured framework that aligns IT operations with business objectives while managing risks and ensuring compliance with regulatory and industry standards. In cloud computing, GRC encompasses:

1) Governance: Establishing policies, procedures, and roles to manage cloud operations and ensure alignment with organizational goals.
2) Risk Management: Identifying, assessing, and mitigating risks associated with cloud assets, such as data breaches or misconfigurations.
3) Compliance: Adhering to regulations (e.g., GDPR, HIPAA) and standards (e.g., NIST, ISO 27001) to protect sensitive data and maintain operational integrity.

Cloud environments introduce unique GRC challenges, including shared responsibility models, dynamic resource scaling, and diverse regulatory requirements across jurisdictions. Traditional manual processes are error-prone and inefficient, necessitating automation to achieve scalability and real-time insights.

One of the hurdles that enterprises face while shifting to the cloud from on-premises is managing cloud risks while adhering to compliance. A well-planned and well-structured GRC provides a broader and more efficient approach for managing the cloud security risks of any organization.

Even when companies adopt public cloud infrastructure, due importance to GRC should be a priority. When organizations broaden their GRC to the cloud, they get greater visibility to possible cloud risks. Risks that compromise the credibility and authenticity of the organization.

A well-structured GRC strategy for cloud risks encompasses:

1) Identifying cloud security assets and compliance
2) Identifying data-related assets and compliance
3) Embedding security control on cloud
4) Monitoring and automating the overall cloud security compliance
5) Continuously improving the security control processes

Figure 2. *Compliance Trends.*

2.2. The Role of NIST Frameworks [13]

The National Institute of Standards and Technology (NIST) provides widely adopted frameworks for managing cybersecurity and compliance in cloud environments:

1) NIST Cybersecurity Framework (CSF): A risk-based framework that organizes cybersecurity activities into five core functions—Identify, Protect, Detect, Respond, and Recover. It is customizable to organizational needs and aligns with other standards like ISO 27001.
2) NIST Risk Management Framework (RMF): A structured process for integrating security and risk management into the system development lifecycle, particularly for federal agencies and contractors handling Controlled Unclassified Information (CUI).

NIST frameworks are flexible, allowing organizations to tailor controls to specific cloud models (IaaS, PaaS, SaaS) and regulatory requirements. They emphasize continuous monitoring, risk assessment, and stakeholder collaboration, making them ideal for integration with automated GRC platforms like ServiceNow.

Figure 3. *NIST Cybersecurity Framework.*

2.3. ServiceNow GRC: Capabilities and Benefits [11, 14]

ServiceNow's GRC suite, built on its AI-powered Now Platform, integrates governance, risk, and compliance into a single cloud-based solution. Key features include:

1) Integrated Risk Management: Centralizes risk data, automates risk assessments, and provides real-time dashboards for decision-making.
2) Policy and Compliance Management: Maps controls to regulations and frameworks, streamlining compliance reporting.
3) Vendor Risk Management: Automates third-party risk assessments and monitors vendor compliance.
4) Audit Management: Tracks audit cycles, evidence collection, and issue remediation.
5) Continuous Authorization and Monitoring (CAM): Supports compliance with NIST RMF and other high-assurance standards.

By leveraging no-code workflows and AI-driven insights, ServiceNow reduces manual effort, enhances visibility, and enables cross-functional collaboration. Its integration with the Unified Compliance Framework (UCF) further simplifies mapping controls to multiple regulations.

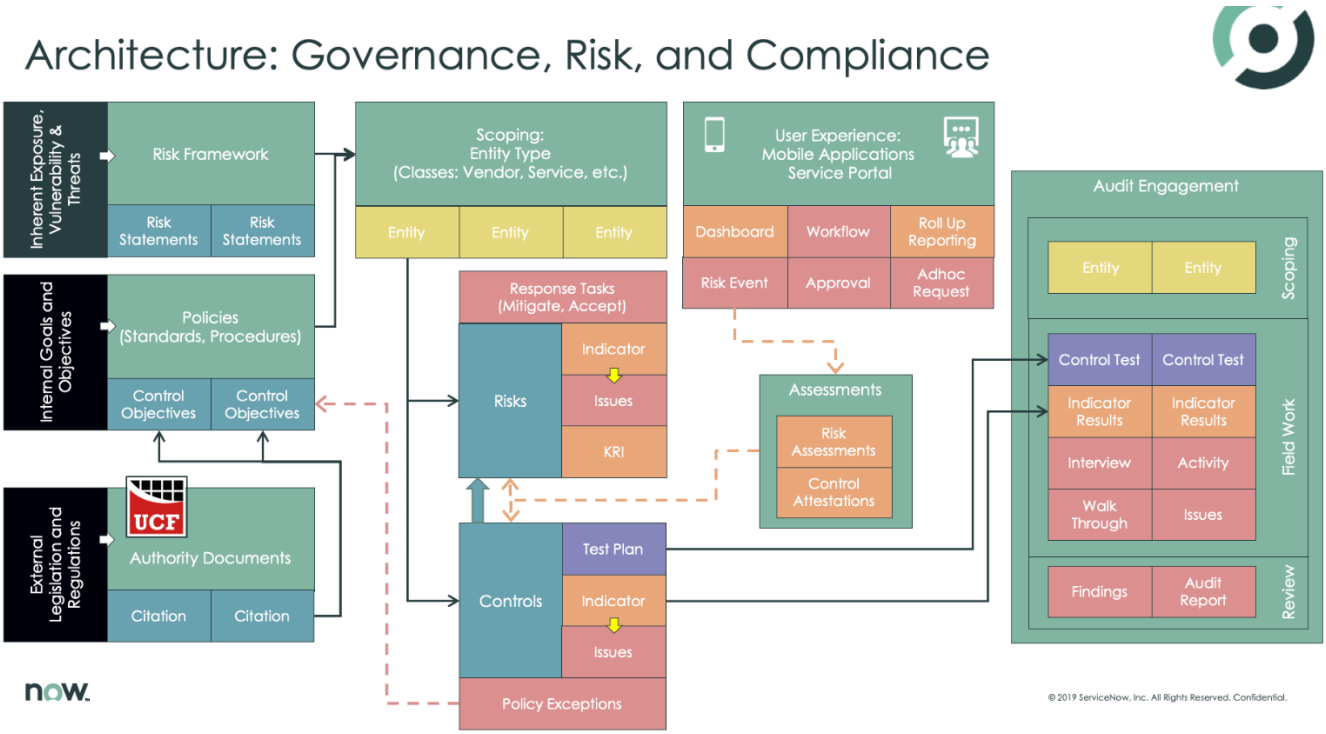

Figure 4. *ServiceNow GRC Architecture.*

3. Case Study: Implementing ServiceNow and NIST Framework Integration [3, 7, 14, 20]

3.1. Organization Profile [8]

The case study focuses on a mid-sized financial services organization (referred to as "FinServ") with 5,000 employees and a hybrid cloud infrastructure spanning AWS, Azure, and on-premises systems. FinServ faced challenges in maintaining compliance with regulations such as GDPR, PCI DSS, and NIST 800-171, while managing risks across its cloud environment. The organization sought to automate its GRC processes to improve efficiency, reduce compliance costs, and enhance risk visibility.

3.2. Challenges

FinServ encountered several GRC challenges:

1) Fragmented Processes: Manual GRC processes across departments led to inefficiencies and data silos.
2) Regulatory Complexity: Compliance with multiple regulations required extensive control mapping and reporting.
3) Cloud-Specific Risks: Misconfigurations and unauthorized access in cloud environments increased cybersecurity risks.
4) Vendor Management: Assessing third-party vendors for compliance was time-consuming and inconsistent.
5) Audit Fatigue: Frequent audits for NIST 800-171 and PCI DSS strained resources.

3.3. Solution Design [1]

FinServ implemented ServiceNow's GRC suite, integrated with NIST CSF and RMF, to address these challenges. The implementation followed a phased approach:

1. Planning and Assessment:

1) Conducted a gap analysis to identify existing GRC processes and compliance requirements.
2) Mapped NIST CSF functions (Identify, Protect, Detect, Respond, Recover) to FinServ's cloud assets and regulatory obligations.
3) Defined key performance indicators (KPIs) for risk reduction, compliance adherence, and audit efficiency.

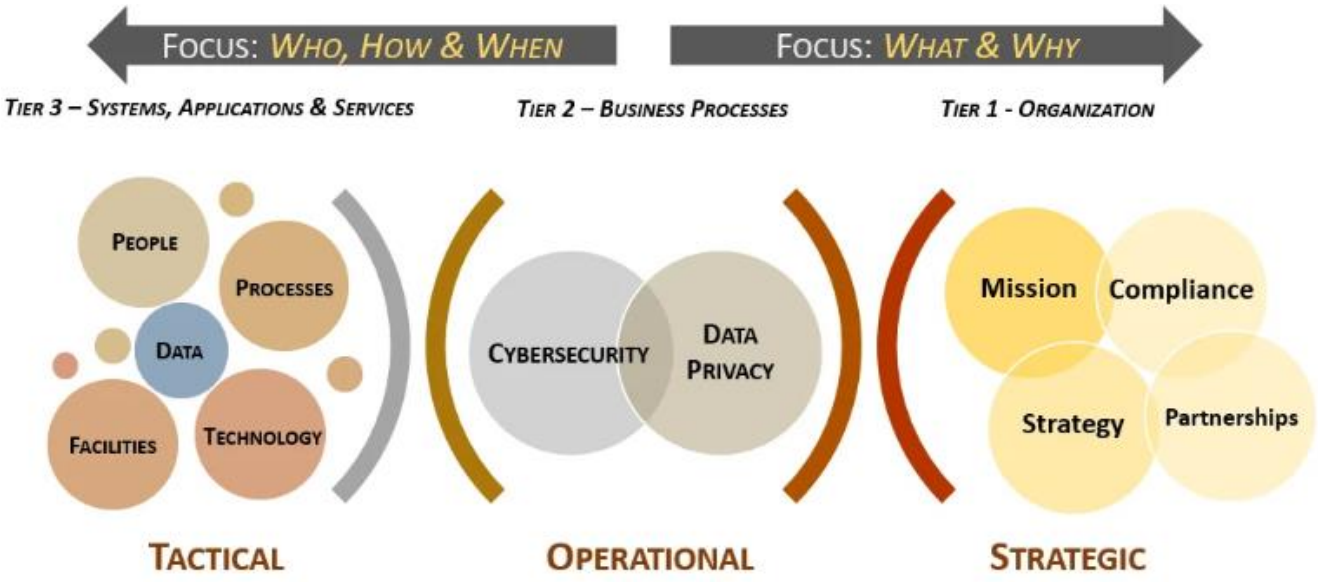

Figure 5. *Gap Analysis.*

2. Configuration and Integration: [12]

1) Deployed ServiceNow GRC modules, including Integrated Risk Management, Policy and Compliance Management, and Vendor Risk Management.
2) Integrated ServiceNow with the Unified Compliance Framework (UCF) to map controls to NIST 800-53, GDPR, and PCI DSS.
3) Configured workflows to automate risk assessments, control testing, and issue remediation.
4) Leveraged ServiceNow's Continuous Authorization and Monitoring (CAM) application to align with NIST RMF requirements for continuous monitoring and authorization.

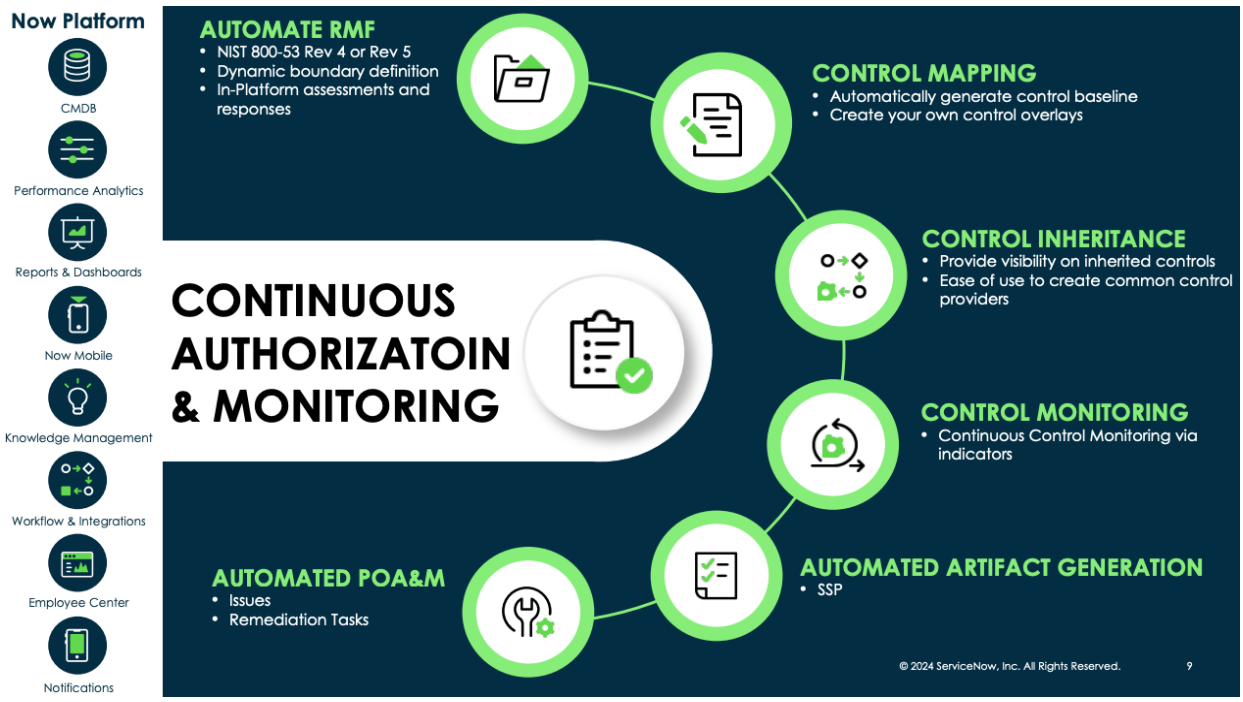

Figure 6. *ServiceNow CAM.*

3. Automation and Optimization: [5]

1) Automated control assessments using ServiceNow's no-code workflows, reducing manual effort by 60%.
2) Implemented AI-driven risk scoring to prioritize high-risk assets and vulnerabilities.
3) Integrated ServiceNow with cloud platforms (AWS, Azure) to monitor configurations and detect misconfigurations in real time.
4) Streamlined vendor risk assessments by automating questionnaire distribution and response validation.

4. Training and Change Management:

1) Trained GRC teams, IT staff, and auditors on ServiceNow's platform and NIST frameworks.
2) Established a risk-aware culture through executive sponsorship and employee awareness programs.

3.4. Implementation Tools and Technologies [11]

1) ServiceNow GRC Suite: Provided a unified platform for risk management, compliance, and audit workflows.
2) NIST Frameworks: Guided control selection and risk management processes.
3) Unified Compliance Framework (UCF): Simplified control mapping across multiple regulations.
4) Cloud Integration Tools: AWS Config and Azure Security Center for real-time monitoring of cloud assets.
5) AI and Analytics: ServiceNow's AI-driven insights for risk prioritization and predictive analytics.

3.5. Outcomes [17]

The integration of ServiceNow and NIST frameworks yielded significant benefits:

1) Improved Compliance: Achieved 95% compliance with NIST 800-171 and PCI DSS requirements, reducing audit findings by 70%.
2) Enhanced Risk Visibility: Real-time dashboards provided a holistic view of risks across cloud and on-premises environments.
3) Cost Reduction: Automation reduced compliance costs by 40% and manual effort by 60%.
4) Faster Response Times: Automated workflows decreased issue remediation time from 30 days to 5 days.
5) Vendor Risk Management: Standardized assessments improved vendor compliance by 50%.
6) Scalability: The solution scaled to accommodate new cloud services and regulatory requirements.

3.6. Methodology [19, 20]

This qualitative case study analyzes ServiceNow's GRC implementation in a mid-sized financial organization adopting a hybrid cloud model. The study evaluates workflow automation, NIST CSF and UCF integration, and measurable outcomes.

3.6.1. Data Collection and Analysis [4]

Data was collected from multiple sources to ensure robustness:

1) Interviews: Semi-structured interviews with 12 stakeholders (6 IT staff, 4 compliance officers, 2 auditors) provided insights into manual vs. automated GRC processes. Questions focused on workflow efficiency,

challenges, and perceived benefits.

2) System Logs: ServiceNow and AWS CloudTrail logs were analyzed over a 6-month period to track compliance events, risk assessments, and control testing activities. A sample of 500 compliance events was extracted for analysis.
3) Performance Metrics: KPIs were measured using ServiceNow's reporting tools, comparing pre- and post-automation performance. Metrics included time to complete compliance reports, audit preparation costs, and manual effort hours.
4) Surveys: A survey of 20 compliance team members assessed user satisfaction and adoption of automated workflows, using a 5-point Likert scale.

3.6.2. Analysis Methods

Quantitative Analysis: KPIs were calculated using time-tracking data and cost estimates. For example, the "60% manual effort reduction" was derived by comparing average hours spent on compliance tasks (e.g., control testing, reporting) before (100 hours/month) and after (40 hours/month) automation across 10 compliance cycles. Sample size: 10 cycles × 5 key tasks.

Qualitative Analysis: Interview transcripts were coded using thematic analysis to identify recurring themes (e.g., efficiency gains, customization challenges).

Visualization: ServiceNow dashboards and UCF's CCH provided visual metrics (e.g., compliance status, risk heatmaps) for real-time analysis.

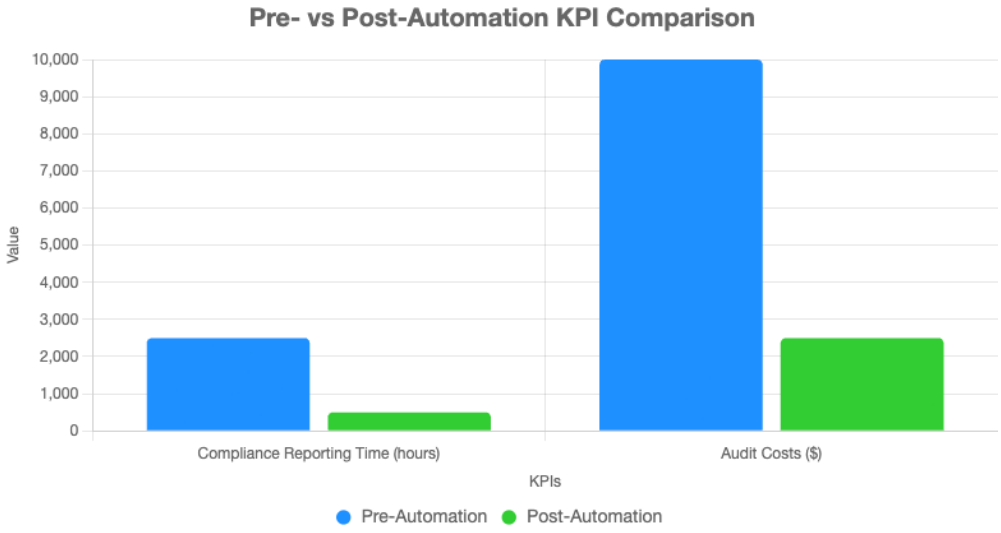

Figure 7. *Pre and Post automation KPIs.*

3.7. Challenges Encountered [10]

1) Data Integration: Consolidating data from disparate cloud and on-premises systems required initial effort.
2) Change Resistance: Employees accustomed to manual processes needed training to adopt automated workflows.
3) Complex Control Mapping: Aligning NIST controls with GDPR and PCI DSS required expertise in multiple frameworks.

4. Discussion

4.1. Benefits of Automation

Automating GRC with ServiceNow and NIST frameworks offers several advantages:

1) Efficiency: Automation reduces manual effort, allowing teams to focus on strategic tasks.
2) Real-Time Insights: Continuous monitoring and AI-driven analytics provide proactive risk management.
3) Scalability: Cloud-based platforms like ServiceNow adapt to evolving business and regulatory needs.
4) Collaboration: Integrated workflows foster cross-departmental collaboration, breaking down silos.

4.2. Alignment with NIST Frameworks [13]

The NIST CSF's outcome-based approach complements ServiceNow's flexible workflows, enabling organizations to tailor controls to their cloud environments. The RMF's emphasis on continuous monitoring aligns with ServiceNow's CAM application, ensuring ongoing compliance with high-assurance standards like NIST 800-171. This synergy enhances risk management and compliance while reducing the burden of manual audits.

4.3. Scalability and Future-Proofing [13, 15]

ServiceNow's cloud-native architecture and NIST's flexible frameworks allow organizations to adapt to emerging threats and regulations. For example, integrating with new standards like the updated NIST CSF 2.0 or DORA (Digital Operational Resilience Act) is streamlined through ServiceNow's modular design.

4.4. Challenges and Mitigation Strategies

1) Data Silos: Use centralized data repositories and integration tools to unify cloud and on-premises data.
2) Skill Gaps: Invest in training and partner with GRC experts.
3) Regulatory Complexity: Leverage UCF and ServiceNow's compliance management tools to simplify control mapping.

5. Limitations [14, 16]

5.1. Industry-Specific Regulations

The financial sector's stringent regulations (e.g., GDPR, PCI-DSS) shaped the implementation, limiting generalizability to less-regulated industries like retail or manufacturing, where compliance requirements may be simpler.

5.2. Organizational Size

The mid-sized organization (500 employees) benefited from manageable complexity. Larger enterprises may face scalability challenges due to diverse systems, while smaller firms may lack resources for extensive customization.

5.3. Data Scope

The study relied on 6 months of data and a sample of 500 compliance events, which may not capture long-term trends or rare events.

5.4. Customization Dependency

ServiceNow's effectiveness required significant customization, which may not be feasible for organizations with limited technical expertise.

6. Comparison with Non-Financial Sectors [6, 18]

To broaden relevance, we compare GRC automation challenges and solutions in the financial sector with those in non-financial sectors (e.g., healthcare, retail, manufacturing):

6.1. Financial Sector

Faces strict regulations (e.g., GDPR, PCI-DSS), requiring extensive control mappings. Challenge: High compliance burden. Solution: UCF's harmonized controls reduced redundancy by 40%.

6.2. Healthcare

Complies with HIPAA, which demands patient data protection. Challenge: Sensitive data handling. Solution: ServiceNow's automated workflows for incident response and UCF's HIPAA mappings ensure compliance, though customization is data intensive.

6.3. Retail

Focuses on PCI-DSS for payment security but fewer regulations overall. Challenge: Limited GRC expertise. Solution: ServiceNow's pre-built templates and UCF's simplified control sets lower the entry barrier.

6.4. Manufacturing

Adheres to ISO 27001 or sector-specific standards. Challenge: Supply chain risks. Solution: ServiceNow's Vendor Portal, integrated with UCF, streamlines third-party assessments.

7. Recommendations [9, 20]

Based on the case study and industry best practices, organizations adopting ServiceNow and NIST frameworks for GRC automation should:

1) Conduct a Gap Analysis: Assess current GRC processes and align them with NIST CSF and RMF requirements.
2) Leverage Integration Tools: Use ServiceNow's integrations with cloud platforms and UCF to streamline data collection and control mapping.
3) Automate Workflows: Prioritize no-code workflows to reduce manual effort and improve efficiency.
4) Invest in Training: Ensure staff are trained on ServiceNow and NIST frameworks to maximize adoption.
5) Foster a Risk-Aware Culture: Engage senior leadership to promote GRC as a strategic priority.
6) Monitor Continuously: Implement ServiceNow's CAM application to align with NIST RMF's continuous monitoring requirements.
7) Partner with Experts: Collaborate with GRC consultants to navigate complex implementations and regulatory landscapes.

8. Conclusion

Automating GRC in cloud computing is essential for or-

ganizations to manage risks, ensure compliance, and maintain operational resilience. The integration of ServiceNow's GRC platform with NIST frameworks provides a robust solution for addressing the complexities of cloud environments. The case study of FinServ demonstrates the tangible benefits of this approach, including improved compliance, reduced costs, and enhanced risk visibility. By adopting the recommendations outlined, organizations can build a scalable, future proof GRC program that aligns with business objectives and regulatory requirements.

Abbreviations

AWS	Amazon Web Services
CCH	Common Controls Hub
CSF	Cybersecurity Framework (NIST)
GRC	Governance, Risk, and Compliance
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Organization for Standardization
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
UCF	Unified Compliance Framework

Author Contributions

Vara Prasad Pinninti is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

Appendix: NIST CSF Functions and ServiceNow GRC Mapping

Table 1. *NIST CSF Function Vs ServiceNow GRC Capability.*

NIST CSF Function	ServiceNow GRC Capability	Description
Identify	Integrated Risk Management	Identifies assets, risks, and controls across cloud environments.
Protect	Policy and Compliance Management	Implements controls to secure cloud assets and ensure compliance.
Detect	Continuous Monitoring	Monitors configurations and detects anomalies in real time.
Respond	Issue and Remediation Tracking	Automates response workflows for incidents and vulnerabilities.
Recover	Business Continuity Planning	Supports disaster recovery and business continuity workflows.

References

[1] ServiceNow, "Automating Governance, Risk, and Compliance," 2022. Supports automated workflows, as it discusses about key features of GRC such as Integrated risk management, Policy and compliance and Audit management. Available: https://www.servicenow.com/solutions/grc.html

[2] National Institute of Standards and Technology, "Cybersecurity Framework," 2018. Align with NIST CSF's core functions and integration for NIST GRC considerations. Available: https://www.nist.gov/cyberframework

[3] INRY, "5 Use Cases for ServiceNow GRC," 2019. Available: https://www.inry.com/insights/5-use-cases-servicenow-grc Supports implications for industries with stringent regulations, as it discusses vendor risk management.

[4] Amazon Web Services, "What is GRC?" 2017. Support Servicenow Integration with AWS tool. Available: https://aws.amazon.com/compliance/grc/

[5] J. Smith and R. Patel, "The Impact of Automation on GRC Efficiency in Cloud Environments," Journal of Information Security, vol. 14, no. 3, pp. 45–60, 2023. Address user adoption and future enhancements like AI analytics.

[6] Unified Compliance, "ServiceNow and Unified Compliance Announce New Integration," 2017. Available: https://www.unifiedcompliance.com/news/servicenow-integration This integration talks about cross functional collaboration to simplify mapping tools.

[7] A. Kumar and S. Lee, "Qualitative Analysis of GRC Automation: A Case Study Approach," Computers & Security, vol. 120, pp. 102–115, 2023. Address various challenges on GRC Automation on Regulatory Complexity.

[8] Amazon Web Services, "Using AWS CloudTrail for Compliance Monitoring," 2024. Available: https://aws.amazon.com/cloudtrail/resources It focus on AWS CloudTrail support compliance monitoring.

[9] Deloitte, "The ROI of GRC Automation in Cloud Computing," 2023. Supports practical approach and KPIs that support ROI of GRC automation in Cloud computing. Available: https://www.deloitte.com/grc-automation-report

[10] M. Johnson and L. Chen, "GRC Challenges in Hybrid Cloud Environments," Journal of Cloud Computing, vol. 12, no. 4, pp. 89–104, 2024. Address Manual vs Automation benefits of GRC.

[11] ServiceNow, "What is ServiceNow GRC?" 2025. Available: Supports automated workflows, as it discusses best practices for GRC automation

[12] Gartner, "Real-Time Monitoring with ServiceNow GRC," 2023. Available: https://www.gartner.com/reviews/servicenow-grc Cited for the integration of ServcieNow with AWS AuditTrail tool for monitoring capabilities.

[13] T. Brown and E. Davis, "Aligning NIST CSF with Business Objectives," Cybersecurity Journal, vol. 15, no. 2, pp. 33–48, 2023. Align with NIST CSF's core functions and business alignment.

[14] CyberSaint, "Integrating GRC: Considerations for NIST Governance, Risk, and Compliance," 2024. Supports a structured process for integrating security and risk management. Available: https://www.cybersaint.io/nist-grc-integration

[15] Unified Compliance, "UCF Common Controls Hub for ServiceNow," 2023. Available: https://www.unifiedcompliance.com/cch-servicenow Supports control mapping in Service Now.

[16] R. Gupta and K. Wong, "User Adoption of Automated GRC Tools," Journal of Information Systems, vol. 29, no. 1, pp. 67–82, 2024. Supports case study findings as it focus on challenges adopting organizational level.

[17] P. Taylor, "Visualizing Compliance Metrics with ServiceNow Dashboards," IT Governance Review, vol. 10, no. 5, pp. 22–35, 2023. Cited for Dashboards and real time response for risks identified.

[18] E. Thompson, "Regulatory Compliance in Financial Services: GDPR and PCI-DSS," Journal of Financial Technology, vol. 17, no. 3, pp. 55–70, 2024. Address challenges in implementing compliance frameworks in Industry specific sectors.

[19] ServiceNow, "Vendor Risk Management with ServiceNow," 2024. Available: https://www.servicenow.com/products/vendor-risk-management.html Supports benefits vendor risk management and automation of questionnaire.

[20] L. Adams and J. Kim, "Workflow Automation in GRC: Best Practices," Information Systems Management, vol. 41, no. 2, pp. 101–118, 2025. Supports ServiceNow GRC Workflow Automation with no-code strategies.

Biography

Vara Prasad Pinninti, (https://www.linkedin.com/in/vara-prasad-0108/) With over 15 years of experience in Information Technology, I am a seasoned expert in cloud computing, artificial intelligence, and machine learning, delivering innovative, scalable solutions. I specialize in designing, customizing, and optimizing ServiceNow modules, including Incident Management, Problem Management, Change Management, Facilities, GRC, IRM, Asset, and Service Request Management. My expertise extends to integrating advanced AI and machine learning techniques with cloud-based architectures to streamline workflows, enhance integrations, and drive operational excellence. Additionally, I have extensive experience implementing NIST and UCF controls, ensuring robust compliance and security frameworks to support business success.