World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Bridging ITSM and GRC: A framework for audit-ready configuration management using service Now

Rashmi Bharathan *

University of Madras, Chennai, Tamil Nadu, India.

World Journal of Advanced Engineering Technology and Sciences, 2025, 16(03), 531-537

Publication history: Received on 15 August 2025; revised on 20 September 2025; accepted on 23 September 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.16.3.1359

Abstract

Information Technology Service Management (ITSM) and Governance, Risk, and Compliance (GRC) are coming together as a critical concern in organisations responsible for service productivity and regulatory requirements at the same time. Configuration management is a key enabler to this alignment, providing visibility into assets and relationships, and reporting requirements. This paper explains why configuration management fills the gap between ITSM and GRC and why it is a good practice to support audit-ready processes by leveraging ServiceNow as the convergence platform. An application reference architecture is proposed that emphasises automated discovery, rich attribute sets for compliance attestation. Coded controls, ongoing monitoring, and audit automation with evidence-based auditing. Implementation challenges such as data quality, siloed organisations, and resistance to change, and critical success factors such as automation, executive buy-in, and staged implementation are discussed. Some of the key takeaways to support the next steps for financial and revenue management automation implementation are adaptive automation, regulatory insights, and sustainability integration. By embedding governance into the way your business operates, ServiceNow enables organisations to continuously ensure IT service delivery resiliency and compliance.

Keywords: ITSM; GRC; Configuration Management; ServiceNow; Audit Readiness

1. Introduction

Enterprises increasingly demand both operational excellence and regulatory compliance. The report emphasizes that achieving these goals requires the effective convergence of Information Technology Service Management (ITSM) and Governance, Risk, and Compliance (GRC) functions. Organizations are increasingly challenged to show that digital infrastructures are secure and demonstrate the integrity of the organization while remaining agile in services. As a result, there has been a strategic push to integrate hardware configuration management into ITSM practices, ensuring that assets, including hardware, software, associated components, attributes, and meta-assets, are properly documented, classified, and monitored. At the same time, GRC requires close controls, the ability to visually see compliance status in real time, and provable audit readiness. Broadly, all these traditionally siloed domains need to get closer associated with one another to enable better control, reduced risk exposure, and greater service reliability [1-3]. The growing complexity of IT environments, coupled with rising cybersecurity risks and evolving regulatory requirements (such as GDPR, HIPAA, and SOX), has made the integration of ITSM and GRC capabilities more essential than ever. Again, this is compared to the cost of reliable services, which are priced at reasonable, money-saving levels. Behind the scenes lies a tightly integrated Configuration Management ecosystem. In principle, this ecosystem can bring ITSM and GRC closer together by providing visibility into assets, their interdependencies, and their compliance status [4, 5].

* Corresponding author: Rashmi Bharathan.

One IT service management cloud solution vendor that markets itself as a strong integrator is ServiceNow. With ServiceNow's built-in ITSM and GRC integrations, organisations have been able to operationalise the enforcement of policies, automate control tests, and aggregate configuration states for auditing and remediation. However, this potential is only possible if there exists a framework that explicitly links these domains in terms of processes, information, and reporting functions [6, 7]. In addition, this paper proposes a holistic model for the concept of a relationship between ITSM and GRC, centred on ServiceNow to supply configuration management infrastructure for auditing. In this paper, we examine how enterprises can harness this synergy by leveraging domain knowledge, compliance requirements, and platform enrichment. These elements serve as predictive enablers for closed-loop compliance monitoring, accelerated audits, and proactive risk management. The added value of the proposed model is most evident in regulated industries such as finance, healthcare, and telecommunications. In these sectors, non-compliance can result in financial penalties and reputational damage, ultimately undermining public trust in the organisation [8, 9].

2. Foundations of ITSM and GRC in Enterprise Environments

To assess how effectively ITSM and GRC can be integrated, it is important to first understand their respective roles within enterprise IT operations. ITSM represents a set of practices designed to deliver business value from IT services by aligning them with organisational goals and enhancing performance through maturity models, as shown in Figure 1. Its primary goal is to ensure that information technology (IT) services are so designed, implemented, and managed that their features and functions match the principles of user expectations and organisational objectives [10, 11].

By contrast, GRC stands for the overall methodology of not only ensuring that organisational operations are aligned correctly with regulatory requirements, but taking a proactive stance towards risk management, while following a standard and repeatable approach to governance. Governance refers to the framework of authority and responsibility that guides decision-making. Risk management involves mechanisms for identifying and mitigating uncertainties. Compliance encompasses the mechanisms required to meet specifications, policies, and regulatory requirements. Taken together, these functions can be employed to build trust, reduce exposure, and enable protection of corporate assets in an unsteady operating environment [12, 13]. Although historically these two disciplines have worked in their own space, there is an increasing recognition of where the ITSM and GRC belong. Threat of failure: Information Technology Service Management (ITSM) processes can introduce risks at any time, as system upgrades or infrastructure changes may create new vulnerabilities or lead to compliance failures if not carefully managed. Regulated entities, in turn, can leverage insights from compliance checks and risk assessments to optimise service delivery. These insights help identify process inefficiencies and uncover potential vulnerabilities within the system. Hence, such a siloed approach results in business process inefficiencies in terms of the gaps, duplication, and loopholes of accountability (especially when, for instance, an audit trail or an incident response event requires cross-system auditing and outcomes) [14, 15].

Thus, the convergence between ITSM and GRC is not only a technology question; it is a business question. Organisations that effectively orchestrate these domains can ensure that changes are not only controlled and documented but also systematically evaluated for their compliance impact. Similarly, adding operating information derived from service management processes to audit trails to provide richness and context for further understanding and interpretation of the issues can also be envisaged [16, 17]. As we'll see in the next section, configuration management is a great tool to leverage when it comes to making this convergence between ITSM and GRC work perfectly. Centralised configuration database serving as one source of truth to support compliance and risk-based decision-making/assessment. Therefore, ITSM and Responsible Care for GRC functions can be configured as part of a configuration process for the goal of audit-readiness and to ensure alignment with audit requirements.

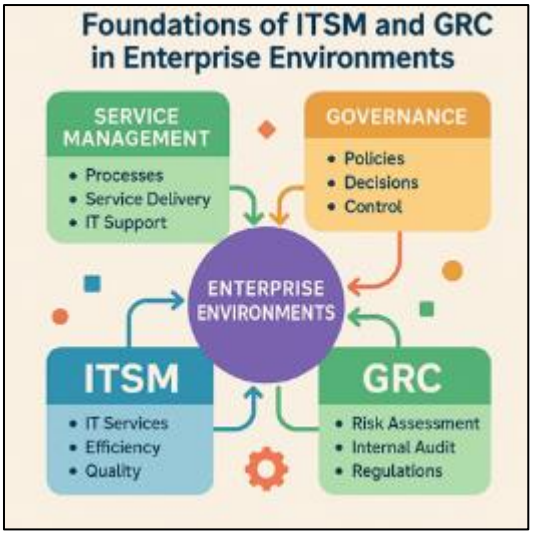

Figure 1 Diagram illustrating the core components of IT Service Management (ITSM) and Governance, Risk, and Compliance (GRC) within enterprise environments, highlighting their interdependencies and foundational roles

3. A Framework for Audit-Ready Configuration Management Using ServiceNow

To connect ITSM and GRC with ServiceNow, we must establish a framework that ties together the configuration management and governance, risk, and compliance processes, both from a functioning standpoint and from a content perspective in the ServiceNow tool. If it can't be mapped to regulatory intent, automating the control enforcer, and being auditable essentially forever, then this architecture also can't do what is required [18]. The typological model given below captures central properties of such a language frame and an abstraction that makes its theoretical use inexpensive and transparent. Automation is achieved through ServiceNow's Discovery and Service Mapping, which perform configuration discovery and normalisation. The CMDB is updated with accurate and current asset data, providing a reliable baseline of configuration items (CIs) and their dependencies. This ensures the persistent accuracy of information and improved visibility across IT services. Clean normalised data is the most important information source for level of services mapping and control provisioning. Next comes compliant attribute enrichment: The ability to map CIs to metadata in a related governance context. Badges and labels in ServiceNow's Policy and Compliance Management module enable regulations, control owners, and risk severity to be mapped directly onto configuration items (CIs). Building on this concept, studies suggest that compliance monitoring and reporting can also be performed directly from the CMDB [3, 4]. By incorporating both regulatory-operational and operational content within the CMDB, a contextual layer is created that enables outcomes to be realised directly within the CMDB itself. During the control implementation phase, both preventive and detective controls should be designed and applied. ITSM workflows, such as change and incident management, need to be configured so that change requests are automatically checked against policy rules. This process can trigger reviews or halt approvals when necessary, thereby embedding compliance directly into the routine tasks of IT operations [5, 6]. Once controls are in place, a continuous monitoring activity watches everything and responds appropriately to exceptions. ServiceNow can connect to vulnerability scanners, patch management tools, and monitoring agents to assess compliance status in real time. And when exceptions happen, that automatically triggers a response for remediation or remediation workflow. The proactive aspect not only serves security/regulatory functions, but it also minimises the need for manual intervention [7, 8].

ServiceNow maintains detailed documentation of changes, control tests, exceptions, and compliance activities for each configuration item (CI). Automating the collection of this information as audit evidence represents the next logical step toward achieving audit readiness. This information is readily accessible for audit reporting, enabling faster and more defensible audit responses. Within the Audit Management module, schedules, assignments, and documentation are completed automatically, eliminating the need for ad hoc processes [9, 10]. This is closely linked to risk prioritisation, which allows you to specify scores to apply to risk and map risks to CIs according to impact and exposure. ServiceNow's Risk Management module is one way of assigning risk levels and including them in ITSM processes for high-risk items to receive the appropriate attention in change approvals/classifications or incident escalations [11, 12].

Control effectiveness, audit, and non-compliance reporting are provided via control visualisation dashboards. These lessons can be extended to include future developmental thinking. Finally, the full real-time view and dashboard allow all stakeholders to assess the actual level of compliance effort [13,14]. Third, governance coupling may help achieve

functional cross-coordination. Executive, compliance, and IT ops will see the right dashboards and reports to get the information they need to do their jobs. This facilitates the process of shared accountability and also helps to internalise audit-relevant awareness as a continuous and systemic (rather than periodic) requirement [15, 16]. With a lightweight framework that automates, unifies, and converges on data, enterprises can progressively implement continuous compliance and audit-ready data. In this way, the CMDB becomes a compliance-aware resource integrated into the ITSM managed desktop and mobile processes and driven by GRC policies. In summary, if organisations can make the transition to this model of compliance, the risk of non-compliance will be minimised; audits will also be simplified, and innovation for IT Service integrity will be accelerated. The first part of the booklet goes beyond simply describing key implementation challenges and success drivers. It also seeks to explore common pitfalls and the underlying dynamics that influence the successful adoption of such a framework.

Therefore, leveraging ServiceNow as an integration mechanism between ITSM and GRC can be highly effective when supported by a well-defined framework. Such a framework should incorporate configuration management best practices alongside governance, risk, and compliance processes. This architecture should maintain identified configuration data correlated with regulatory goals, automate the control enforcer, and be audit-capable at all times. Furthermore, individuals and organisations concerned with privacy recognised the value of the combined conceptual and measurement framework. To complement the narrative description, the key contributions and mediated value of each step in the framework are summarised in Table 1.

Table 1 Stages of Audit-Ready Configuration Management Framework in ServiceNow

Framework Stage	Key Activities	Primary Value
Configuration Discovery & Baseline	Use ServiceNow Discovery and Service Mapping to populate and normalise the CMDB.	Ensures accurate, up-to-date data for compliance foundations.
Compliance Attribute Enrichment	Link CIs to regulations, policies, ownership, and risk ratings.	Embeds governance context into operational data.
Control Implementation	Embed preventive and detective controls into ITSM workflows.	Proactively enforces compliance during routine IT operations.
Continuous Monitoring & Exceptions	Integrate monitoring tools for real-time compliance checks and trigger workflows.	Enables early detection and remediation of non-compliance.
Automated Evidence Documentation	Generate audit trails, test results, and compliance records through the Audit module.	Simplifies audit preparation and strengthens defensibility.
Risk Prioritization	Apply risk scoring to CIs and link to ITSM processes.	Focuses attention on high-impact systems and activities.
Compliance Analytics & Reporting	Provide dashboards and role-based reports for stakeholders.	Improves transparency, decision-making, and accountability.
Governance Alignment	Align IT, compliance, and executive oversight with shared metrics.	Embeds audit readiness as an enterprise-wide responsibility.

4. Strategic Recommendations and Future Directions

The challenge with matching ITSM and GRC with ServiceNow is to establish a framework to align the configuration management and governance, risk, and compliance process - both from a functional perspective and from a content perspective within ServiceNow, as shown in Figure 2. This architecture should also allow mapping configuration to regulatory intent, automate the control enforcer, and be auditable down to the nth degree. The typological model that we introduce below captures salient properties of such a framework in an abstraction that is easy and transparent in its use. Clean data is the most important data source for compliance mapping & control deployment [1, 2]. This is followed by profile adherence enrichment, which involves Configuration Items (CIs) with metadata for governance purposes, for example, through badges, labels, tags, and operational records. Studies have noted that this approach could evolve into regulatory-automated compliance. Outcomes could then be triggered directly from the CMDB by leveraging the regulatory-operational content it contains, along with control rules, risk severity, and related attributes mapped directly onto each CI. In designing and implementing preventive and detective controls, ITSM workflows, such as change and incident management, should incorporate automated rule vetting. This ensures that change requests are automatically checked against policy rules, prompting reviews or halting approvals when necessary. Compliance

becomes part of the work and an ongoing activity, watching everything and reacting to exceptions. ServiceNow integrates with scanners, patch management systems, and monitoring systems to determine compliance status in real time. And when deviations do happen, automated remediation or remediation workflows get triggered. As a result, proactive monitoring not only helps to enforce security or regulatory requirements but also decreases the need for human interaction [7, 8].

ServiceNow also hosts the audit trail of changes, control checks, exceptions, and compliance activity that occurs within each CI; an automated service for collecting audit evidence for audit preparedness. The information is easily reportable for audits, enabling faster and more defensible audit responses. Within the Audit Management module, schedules, assignments, and documentation are fully automated, eliminating the need for ad hoc processes [9, 10]. This is closely coupled to risk prioritisation, which allows you to define scores to assign to risk and map risks to CIs based on impact and exposure. ServiceNow's Risk Management module provides a structured approach for classifying risk levels within ITSM processes. It helps identify high-risk items that require greater attention during change approvals or incident escalations [11, 12]. Control visualisation dashboards provide insights into control effectiveness, audit outcomes, and non-compliance reporting. These insights can then be used to support preparation for continuous improvement initiatives. A comprehensive real-time wizard enables compliance initiatives to be quantified and visualised at the enterprise-wide level for all stakeholders. Furthermore, functional coordination may emerge through governance coupling. Role-based dashboards and reporting provide executives, compliance teams, and operations staff with the information they need to perform their roles effectively. This approach encourages shared ownership and reinforces the philosophy that auditing should be viewed as an ongoing, organisational imperative rather than a periodic, individual one [15, 16]. A small-footprint solution that connects, centralises, and automates ensures ongoing data integrity and continuous auditability. In essence, applying this conceptual maturity enables organisations to mitigate regulatory compliance risks, simplify audits, and accelerate innovation. It also transforms the CMDB into a compliance-aware entity, supporting ITSM-enabled practices across both desktop and mobile environments. The first half of this booklet aims to move beyond a simple description of key implementation issues and lessons learned. It also seeks to provide a deeper understanding of common pitfalls and the driving factors that contribute to the successful application of this type of framework.

If activities are guided by a defined framework, they can be aligned more effectively. Such a framework should include configuration management best practices as well as governance, risk, and compliance practices. With this foundation in place, ServiceNow has a strong potential to act as the bridge, serving as the glue between ITSM activities and GRC activities. This architecture needs to have some sort of captured configuration information related to regulatory goals, it needs to be able to automate the control enforcer, and it needs to be ready for the audience at any time. Furthermore, Stakeholders, including business leaders, compliance teams, and data custodians, recognized the value of the integrated conceptual and measurement framework. For ease of reference, Figure 2 summarizes each step's rationale and contribution.

Figure 2 Visual representation of the strategic planning process, illustrating how analysis informs recommendations, which guide actionable plans and shape future directions

5. Conclusion

As digital infrastructures grow more diverse in shape, scale, and complexity, the demands on enterprise architecture also become more sophisticated. This shift reinforces the growing need for unified identity management across complex regulatory environments. At this intersection, ITSM and GRC can converge through audit-ready configuration management. As a result, configuration management, when powered by ServiceNow's unifying platform, must evolve beyond its role as an operational discipline. It should transform into a governance enabler with direct impact on compliance, risk mitigation, and audit simplification. As illustrated in the described frame of reference, the CMDB offers inherent capabilities such as automated discovery, extended compliance, in-line controls, and continuous monitoring. Together, these features position the CMDB as the central focus for enterprise-wide compliance intelligence. Success becomes attainable when strong governance, automation, training, and a phased adoption strategy address challenges such as data quality issues, organisational silos, and tool complexity. Ultimately, the most effective way to manage today's IT environments is to align ITSM and governance processes through ServiceNow. This alignment delivers business visibility, agile governance, and the resilience needed to stay ahead of audits.

References

[1] De Albuquerque JP, Krumm H, de Geus PL, Jeruschkat R. Scalable model-based configuration management of security services in complex enterprise networks. Software Pract Exp. 2011;41(3):307-38.

[2] Whyte J, Stasis A, Lindkvist C. Managing change in the delivery of complex projects: Configuration management, asset information and 'big data'. Int J Proj Manag. 2016;34(2):339-51.

[3] Oluoha OM, Odeshina A, Reis O, Okpeke F, Attipoe V, Orieno OH. Artificial Intelligence Integration in Regulatory Compliance: A Strategic Model for Cybersecurity Enhancement. 2022.

[4] Berlato M, Binni L, Durmus D, Gatto C, Giusti L, Massari A, et al. Digital Platforms for the Built Environment: A Systematic Review Across Sectors and Scales. Buildings. 2025;15(14):2432.

[5] Hjort-Madsen K. Enterprise architecture implementation and management: A case study on interoperability. In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). IEEE; 2006. p. 71c-71c.

[6] Ogunwole O, Onukwulu EC, Joel MO, Adaga EM, Ibeh AI. Modernizing legacy systems: A scalable approach to next-generation data architectures and seamless integration. Int J Multidiscip Res Growth Eval. 2023;4(1):901-9.

[7] Waizenegger T, Wieland M, Binz T, Breitenbücher U, Haupt F, Kopp O, et al. Policy4TOSCA: a policy-aware cloud service provisioning approach to enable secure cloud computing. In: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer Berlin Heidelberg; 2013. p. 360-76.

[8] Emeihe EV, Nwankwo EI, Ajegbile MD, Olaboye JA, Maha CC. The impact of artificial intelligence on regulatory compliance in the oil and gas industry. Int J Life Sci Res Arch. 2024;7(1):28-39.

[9] Gökalp E, Martinez V. Digital transformation maturity assessment: development of the digital transformation capability maturity model. Int J Prod Res. 2022;60(20):6282-302.

[10] Dener C, Nii-Aponsah H, Ghunney LE, Johns KD. GovTech maturity index: The state of public sector digital transformation. Washington, DC: World Bank Publications; 2021.

[11] Moyón F, Méndez D, Beckers K, Klepper S. How to integrate security compliance requirements with agile software engineering at scale? In: International Conference on Product-Focused Software Process Improvement. Cham: Springer International Publishing; 2020. p. 69-87.

[12] Getter JR. Enterprise architecture and IT governance: A risk-based approach. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE; 2007. p. 220.

[13] Cinar B. The role of cloud service brokers: enhancing security and compliance in multi-cloud environments. J Eng Res Rep. 2023;25(10):1-11.

[14] Mahant R, Bhatnagar S. Strategies for Effective E-Governance Enterprise Platform Solution Architecture. Strategies. 2024;4(5).

[15] Patón-Romero JD, Baldassarre MT, Rodríguez M, Runeson P, Höst M, Piattini M. Governance and management of green IT: a multi-case study. Inf Softw Technol. 2021;129:106414.

[16] Henderson K, Pahlenkemper G, Kraska O. Integrated asset management–an investment in sustainability. Procedia Eng. 2014;83:448-54.

[17] Regueiro C, Seco I, Gutiérrez-Agüero I, Urquizu B, Mansell J. A blockchain-based audit trail mechanism: Design and implementation. Algorithms. 2021;14(12):341.

[18] Chakir A, Chergui M, Andry JF. A smart updater IT governance platform based on artificial intelligence. Risk. 2020;8:9.