International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Automating IT Audit Evidence Collection: Reducing Risk and Cost Through ServiceNow Integration

Rashmi Bharathan *

University of Madras, Chennai, Tamil Nadu, India.

International Journal of Science and Research Archive, 2025, 16(03), 1393-1401

Publication history: Received on 02 August 2025; revised on 07 September 2025; accepted on 12 September 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.3.2584

Abstract

The introduction of hundreds of IT infrastructures, as well as the increased regulatory pressures, makes the manual collection of audit evidence inefficient, error-prone, and costly. Reduce Compliance Risk and Lower Operating Costs: Automating the ServiceNow evidence assessment Process for Maintenance and Audit Readiness is a game-changer for reducing compliance risk as well as lowering operating costs. This article discusses the limitations of traditional evidence collection processes and highlights how automation can help you accomplish a higher level of efficiency, accuracy, scalability, and risk reduction. Accordingly, it suggests a framework for an automated and audited ServiceNow-based identity automation solution that performs automated service configuration discovery, followed sequentially by enforcing compliance mapping controls, and ongoing audit and monitoring. The paper also addresses technical and operational issues of implementation, including questions of quality and completeness of data, how to integrate the disparate processes and culture, and how successful implementations have common elements, such as executive sponsorship, automation, training, and incremental implementation. Based upon those findings, some recommendations are proposed for future directions in regard to interoperability, adaptive automation, review based on risk, and sustainability of computer auditing. By integrating compliance into all aspects of daily IT Service management, organizations will progress from reactive audit to proactive governance to build healthier and more resilient and, importantly, more cost-efficient digital ecosystems.

Keywords: IT Audit; Servicenow; Compliance Automation; Risk Management; Evidence Collection

1. Introduction

Within today's digital enterprise, the need for reliable IT audits has never been more important due to greater regulation, sophisticated cyber risks, and stakeholder expectations. In plenty of ways, most traditional IT audits are still over-reliant on the paper trail, while this may provide adequate evidence, it is time-intensive, costly, and prone to measurement error. This manual process is exerting heightened demands on organizations operationally and exposes the organization to compliance risk. As the deployment of business processes continues to expand across cloud-based, hybrid, and distributed infrastructures, manual audit-driven approaches are no longer sufficient to provide timely, accurate, and continuous compliance assurance [1, 2].

Automated evidence collection is a game-changing technology solution that helps to address these challenges by bridging gaps between compliance and governance with ITSM processes. By automating the capture, verification, and reporting of evidence, organizations can significantly reduce the time and cost of audit, whilst providing an improved control environment. In particular, a popular ITSM and GRC tool, ServiceNow, comes with a federated environment to extract audit evidence automatically from: Configuration items, Incident history, Change history, and Compliance monitoring for information security. With a single data location and a unified source for auditors to verify, silos are

* Corresponding author: Rashmi Bharathan

effectively reduced, and duplicate data is eliminated. This approach also ensures that stakeholders ultimately receive the accurate information they need [3, 4]. Further evidence highlights why this has become so important. Regulatory frameworks such as SOX, HIPAA, GDPR, and ISO 27001 impose stringent requirements for controls, traceability, and proof of compliance, along with the need for real-time visibility into IT controls. Compliance violations can result in legal fines, lawsuits, reputational damage, and other consequences [5, 6]. At the same time, organizations face pressure to keep operational costs low, often by limiting internal overhead. Both objectives can be achieved through mechanisms that streamline the collection of audit evidence, for example, using ServiceNow. In this way, compliance assurance can be managed externally while minimizing the significant resource burden internally

Despite all positive aspects of this kind of model, there are certain problems connected with the massive implementation of automation technologies. These involve scalability among various systems; data integrity; the dynamic aspect of the evidence supporting activities within the supply chain, as well as tailoring autopilot activities to an organization's culture. Along with that, IT trust management of ServiceNow should be leveraged prudently; tactical application of the IT role of ServiceNow to its automation, audit evidence potential needs, disciplined thinking in the design of the ontology, and engaging the stakeholders actively at the very beginning of an audit automation initiative, and remaining process-centric [7, 8]. This article presents an overview of ServiceNow's approach to automated capture of IT audit evidence as part of an enterprise governance framework to reduce costs and minimize risk. It begins by explaining why traditional methods of evidence capture are limited-and then goes on to explain the benefits of automation. It then identifies how ServiceNow enables these advantages by outlining the relevant modules and capabilities. A proposal for an inventory of automated sources of audit evidence is presented, followed by a discussion of the issues around automated adoption and key enablers of success. Finally, recommendations and future directions for the development of robust and compliant audit ecosystems in organizations are provided [9, 10].

2. Limitations of Traditional IT Audit Evidence Collection

The traditional approach to IT audit evidence gathering requires significant manual effort to gather, verify, and display IT control and configuration artefacts, as shown in Figure 1. Oftentimes, auditors ask IT personnel for spreadsheets, IT systems logs, change management documents, and access control lists. The IT personnel compile and package these documents for the audit team to analyze. This type of working is no longer able to properly answer the complex reality that larger and modern enterprises require: IT infrastructures have become so big [11, 12], in addition to the many compliance requirements.

Slow and inefficient, manual data collection is a time-consuming process that remains one of its biggest challenges. Consequently, retrieving data across different systems, connecting different data sources, and analyzing the data completeness and accuracy are time-consuming and labor-intensive tasks. Across most organizations, IT teams are often called upon to put out audit-related fires. This requires diverting resources away from business-as-usual activities. Such inefficiency leads to higher audit costs and wasted productivity [13]. A connected issue and problem is that the information is unfavorable and unsound. In many situations, various kinds of information are gathered in various ways by ad hoc processes within a variety of systems, and therefore, a large volume of information is consistently gathered at random. Conformance may be recorded at different levels, such as operational, system, customer, or political. In some cases, auditors may also use different systems to generate relevant and reliable audit evidence. Under these conditions, the reporting process is not simply a frustrating exercise for auditors. Likewise, the identification of audit findings by the organization’s auditors is not diminished [14].

The traditional evidence collection is also retrospective; the evidence is taken on a periodic (Quarterly/Auditing/Incident basis) and not on an ongoing basis. This leaves audits vulnerable to compliance blind spots, which expose organizations to undetected compliance failures or control violations. When non-compliance is ultimately detected, incident damage may have already occurred, both in the form of regulatory fines and on the operational side [15]. Second, the manual aspects make it very difficult to scale. Most organizations are transitioning to multi-cloud and hybrid digital; however, as with most variations on a theme, the depth and breadth of evidence needs increase exponentially. An automated workflow is needed with such a scale, and with the clients' requirements, in recent years, to obtain assurance for controls in near real-time, if not real-time [16]. It is also what makes organizations susceptible to human error - and to fraud or embezzlement. Slippages, omissions, and outright fabrications are only some of the many ways in which an audit process can lose its integrity. These weaknesses cannot be sustained in today’s industry environment. They expose organizations, especially those under close regulatory oversight, to severe legal and economic consequences. The risk is growing as more industries come under stricter regulation [17]. Nevertheless, deficiencies within traditional methods reveal the strong necessity of a more reliable, dependable, and effective audit solution to process evidence. This represents a significant hotspot for automation. The solution demonstrates the types of benefits that capture automation aims to deliver, particularly in counterbalancing capture failures. It also addresses

issues of imprecision, unreliability, and the uneven distribution of capture risk.

Figure 1 Diagram highlighting the key limitations of traditional IT audit evidence collection, including time consumption, manual processes, scattered data, and lack of automation

3. Benefits of Automating IT Audit Evidence Collection

Automation offers solutions to optimize procedures, enhance audit efficiency, and improve overall audit effectiveness. In doing so, it provides businesses with an invaluable remedy for the flaws inherent in manual audit processes. Beyond improving efficiency, automation enables organizations to become smarter in managing regulatory and operational risks. For this reason, it is essential to embed automation as an integral part of IT service and governance processes. In areas where such convergence is beneficial, ServiceNow provides an integrated solution. This commercial off-the-shelf (COTS) offering combines ITIL-based IT service management with smart governance, risk, and compliance (GRC) capabilities.

Among the clear benefits of automation are productivity gains, particularly in evidence collection. Automated workflows collect and store relevant evidence such as change history, incident logs, access control logs, and vulnerability scans within ServiceNow workflows. As a result, manual operators no longer need to perform these functions. This removes the need for audit teams to hunt for data scattered on different systems. Alternatively, there is evidence readily available, reducing the time needed to prepare for an audit from weeks to days, or even hours [15-18]. Closely related to efficiency is the fact that costs are reduced. Traditional audits require huge amounts of human resources to collect, verify, and report on the facts. By automating the collection of data points and evidence instead of manually generating quotes, organizations minimize labor costs and free their IT teams to spend time on value-adding activities. In addition, because there is more verification time required for manual evidence that is fragmented or not enough, audit firms typically charge more for the excessive work and time required to verify. Hence, automation reduces unpredictability and thereby reduces waste and costs to the manufacturing concern [19].

In addition, automation provides increased accuracy and efficiency in audit evidence. Since it gets information immediately from source systems in real time, there is no risk of differences between them; it will no longer be outdated information, and subjective judgment will not occur. For example, automated change management recording in ServiceNow can document when a change was made, when it was approved, and who implemented it, unlike unverifiable 'we said' stories recalled years later. This reliability strengthens the organization's audit posture and provides maximum confidence and assurance to auditors and third parties [20]. Also good here is the differentiation of the ontogenetic developmental transition from exceptional compliance to continuous compliance. Traditionally collected evidence results in point-in-time evidence of compliance, which will give blind areas between audits. Automation brings resiliency into the eyes of controls monitoring and, over time, shapes system compliance status as systems evolve. ServiceNow, also using vulnerability management tools, provides an example in which configuration out-of-compliance is detected during runtime, and a service management tool logs this as audit evidence. This capability enables the detection of control errors at an early stage of the process, before they may have a regulatory consequence [12, 14]. With automation, a more traceable and transparent audit is possible: All evidence found in ServiceNow can be linked to configuration items, policies, and controls. That then automatically builds a clear chain of thought on which auditors can follow a regulatory requirement to its corresponding control test or system provision. This highlights that

transparency delivers two key benefits: it reduces tensions during the audit process and ensures that compliance outcomes are clearly demonstrated in line with required standards such as SOX and GDPR [2-6].

It is additionally a massive advantage in the scalability aspect of automation. The application of hybrid-cloud and multi-cloud systems multiplies the associated metrics, auditable assets, and reports associated with the audit evidence. It also implies that the old habits of work are no longer sustainable. Since they are created natively in ServiceNow, when completely integrated, the automated solutions can scale to map what is known among thousands of assets or processes without any additional overhead. Consequently, audit readiness is eventually delivered with or without the complexity or amount of IT situations [3]. A third added value is that of risk reduction. Businesses avoid the possibility of human error, oversight, or calculated misrepresentation of evidence by automating collection tasks with best practice levels of compliance controls built into your workflow. Furthermore, this approach is grounded in unrelenting vigilance to prevent non-compliance and minimize recovery needs. When breaches are detected, it ensures recovery occurs as quickly as possible, reducing the risk of regulatory sanctions and negative exposure. Consequently, audit is further proactive because the process of risk treatment is generally perceived as a reactive activity [2-4], whereas audit may be regarded as a proactive activity in the context of risk management.

Lastly, more room to be curious (points of intersection between IT and compliance worlds) becomes possible due to automation. Ideally, compliance should not be treated as a manual side activity but as an integral part of standard ITSM processes, such as incident resolution or change requests, something carried out as a full-time responsibility. Consequently, this alignment will remain useful to IT and compliance professionals to reduce friction between the two functions, ensure increased cross-function collaboration, and ensure that compliance goals assist organizational business goals [15]. And that is one of the reasons why automation is becoming an unavoidable component of current audit preparedness in organizations of all scales. Therefore, a necessity for appropriate technological infrastructure to receive such benefits.

4. Service now as a Platform for Automated Audit Evidence Collection

To make new achievements in automation, however, a platform is required to expand and assemble workflows, to introduce controls to monitor them, and to centralize evidence that drives them. ServiceNow is increasingly positioning itself as a platform that unifies ITSM, configuration management, and GRC within a single ecosystem. According to Montag, its flexible data model and strong automation capabilities reinforce King's view that COBIT is particularly effective in ensuring that audit-conscious IT processes evolve into standard IT functions. One of the most important elements of the success of ServiceNow is the Configuration Management Database (CMDB) as a single source of truth for all configuration items (CIs) and their relationship with others (inter-relationship). Since the majority of audit requirements relate to records of system state, change, and privilege, the CMDB is the foundation of documenting evidence. By combining discovery, exploration, and expert features in ServiceNow, the CMDB can automatically track configuration changes across IT infrastructure, applications, and services. These records provide audit evidence that reflects the current configuration being delivered [16].

ServiceNow Policy and Compliance Management builds on that foundation by mapping external regulations, internal policy, and control goals directly to CIs and IT services. One can define breach tests as part of the legislation discovery system to test compliance continuously and save compliance test results as structured audit evidence. For example, indicators such as password policy strength or patch compliance can be periodically tested through automated methods, with the results stored for audit purposes. This eliminates the need for manual reviews of compliance and will provide uniform documentation [17, 18]. Another level of granularity within the platform is achieved by using the Risk Management module, when risks link directly to the capture of evidence. Any risk identified from an audit or monitoring (for example, outdated patches or privileged accounts with unconstrained access) can be automatically recorded and scored in ServiceNow. For auditors, this linkage provides contextual intelligence about not only whether controls exist, but also how well they are achieving their intended purpose (i.e., mitigating a particular risk). Within the ETL, we provide support for risk-based audit, which has gained popularity in the audit industry and government. ServiceNow also offers an Audit Management module for an easy audit process. Audit tasks can be assigned, scheduled, and tracked within the platform, and evidence can be automatically pulled from integrated ITSM and compliance modules. This reduces the administrative burden of audits while keeping data completeness, data consistency, and central exhibit management. In ServiceNow, once audit trails are generated, they are tamper-proof and thus give confidence to auditors with regard to the validity of the sources [9].

Hence, the second benefit is that integration is possible. ServiceNow integrates with external systems (vulnerability scanners, identity and access management, and cloud service providers). Data captured by these tools can be sourced into the CMDB and ServiceNow's compliance framework, providing a unified view of data from multiple sources. This

interoperability ensures that the focus of the audit evidence spans across the entire IT ecosystem, including systems managed by third parties, such as cloud hosts. Together, these characteristics make ServiceNow a powerful provider of automated audit evidence collection. However, successful adoption requires a formal framework matching organizational processes to the capabilities of the platform.

5. A Framework for Implementing Automated Audit Evidence Collection in servicenow

While ServiceNow is able to deliver the technological backbone for automation, it needs a structured and phased framework to deliver its full potential. This creates a situation where the process of collecting and navigating audit evidence remains a technical improvement rather than evolving into a sustainable organizational capability. The approach provided below ties discovery, compliance mapping, control enforcement, monitoring, and reporting together into a continuous loop, turning ServiceNow into the driving force behind audit readiness. The first step is to get a good baseline of configuration. ServiceNow's Discovery and Service Mapping products automate the identification of configuration items (CIs) across the IT infrastructure. They ensure that these items are used to populate the CMDB (Configuration Management Database) with accurate and up-to-date data. This baseline is needed for the purpose of auditing, because it represents ultimate, ground-truth information as to what systems exist, who owns them, and how they interconnect with each other. Without this step, automation runs the risk of being developed on less-than-complete and inaccurate data that reduces audit credibility [11, 12]. Once the baseline is in place, organizations turn to compliance attribute mapping. Each CI needs to be supplemented through governance-related metadata, including relevant regulatory requirements, associated risk ratings, and attributes describing control ownership. ServiceNow's Policy and Compliance Management module provides the means to perform this mapping by associating policies with operational assets. For instance, a database that contains personal health information would be identified with HIPAA requirements, and an application that processes financial reporting would be identified with SOX controls. By including compliance metadata within the CMDB, organizations will ensure that evidence collection is both contextual and comprehensive [10-13].

The third pillar of the framework is to incorporate controls into ITSM processes. Automated compliance checks can be added to ServiceNow workflows for incident, change, and problem management. For example, an automated policy validation could be used in conjunction with a change request sent to a production server to validate that the patch meets approved baselines. If the validation fails, then the workflow can restrict implementation or escalate to a compliance officer. This provides for compliance framing that takes place proactively at the time of IT day-to-day operations as opposed to compliance framing that occurs afterward/subsequently [14]. The framework then progresses to evidence capture with controls embedded that continuously monitor developments. ServiceNow is integrated with monitoring and vulnerability scanners to automatically test controls against real-time data. Non-compliance events are reported automatically and without human intervention to create audit logs. Exceptions are managed in predefined workflows that will delegate into ownership, with workflows for remediation, tracing, and closing the loop with a written fix. The advantage of longitudinal monitoring is that it gives auditors dynamic access to evidence, as audit records are created and validated continuously rather than captured as static snapshots [15, 16].

Monitoring for the Framework is an essential component of the framework, with automatic documentation and storage of evidence. With ServiceNow Audit Management, you can create a single repository from audit trails from ITSM workflow, third-party vulnerability scans, and monitoring. Time, source, and context are all placed on each piece of evidence for a tamper-proof store. The platform can automatically generate reports within seconds when asked by a group of auditors for proof, which saves a lot of time and preparation cost while ensuring standardization. The byproduct of this capability is that audits can transform from reactive functions that are expensive and unreliable to routine validation functions [17]. This documentation is also combined with a risk management function. Risks captured in ServiceNow's Risk Management are being associated with a Configuration Item and an associated Compliance record. For example, a vulnerability with no patch available would not only be reported as Non-Compliant but also get a score for Business impact. Utilizing audit controls is a risk-based data collection strategy that provides not only an understanding of whether controls are in place, but also how the controls specifically mitigate material risk. Linking risk management and audit evidence is also consistent with the current auditing standards that place risk-focused techniques as the inverse of the center of the audit [16-18].

The final element of the framework is reporting and analytics, which ensure governance alignment. ServiceNow dashboards serve as a project-based solution, delivering real-time visibility into compliance, control effectiveness, and auditability across both local and enterprise levels. With role-based access, everyone in the organization, from technical and governance teams to executives, can access the data most relevant to them. Key metrics such as control pass rates, exception closure times, and audit cycle times are tracked as part of a continual improvement plan. This transparency is not only used for audit purposes but also helps to have good governance as it affects responsibility for compliance at

all company levels [19]. Together, these stages create a closed-loop process from discovery to rediscovery. This process enables SOC compliance mapping based on discovery, supports operational delivery, ensures continuous validation through monitoring, and prioritizes audits using risk management. ServiceNow supports this cycle, both as the operations engine and compliant database that keeps audit preparedness from being an interim step, but the status of the organization. Even if your framework is in place, you need to accept that it is not easy to implement a plan. The final section of the article summarises the most common hurdles that prevent the automation of evidence collection for much of the auditors' work, and also the success factors that dictate whether such projects will actually deliver on the promises they make.

6. Implementation Challenges and Success Factors

While the value of automation is clear, adopting automated audit evidence gathering is not always straightforward. The process is often challenged by technical, cultural, and regulatory obstacles. To overcome these, organizations must ensure ServiceNow is implemented in a way that unlocks its full potential. One of the primary hurdles in resolving CMDB-related challenges is maintaining data quality. Automated evidence collection is only as reliable as the underlying configuration data. Unfortunately, many organizations struggle with outdated, incomplete, or poorly maintained CI records, which undermine trust in their audits. Thus, the definition of good discovery practice and the implementation of data stewardship roles may be items that need to be considered as critical success factors [20]. One of them can be the difficulty of integration. As much as ServiceNow is well integrated with many different providers and avenues, there are many ServiceNow clients that are not where they should be with their ServiceNow filters connected to external monitoring, security, and legacy systems without ServiceNow experience and customization. In addition to these gaps, missing evidence can be highly disconcerting for auditors, often resulting from poorly designed interactions that produce contradictory outcomes or leave parts of a query incomplete. Historically, quick-fix solutions were commonly applied to high-risk systems during the early stages of experimentation, typically on a minimal scale, before being progressively and steadily expanded.

Coupled with these technical problems are cultural problems that hamper adoption. One of the challenges arises when controls impose significant overhead, creating what can be termed as inconvenience. Over time, this shapes an ‘auto-mindset’ within IT organizations, where compliance automation is perceived as obtrusive or obstructive. The key to overcoming this resistance lies in clearly describing the benefits of automation and demonstrating potential savings in both cost and time per unit. Automation should be positioned as a way to make work easier, not harder, particularly within production processes. When compliance checks are integrated into existing workflows, pushback can be reduced, and adoption becomes smoother. Then come other regulations that have been on the rise. The requirements of audit specification vary between and within different jurisdictions and among different frameworks, and are continuously changing. ServiceNow should be configured to flex in a technically and humanly cooperative fashion between compliance officers and IT admins. Other key success factors include having an executive sponsor with delegated authority, ensuring sufficient resources to sustain implementation, and providing role-based training. Such training helps clarify the roles and responsibilities of different stakeholders in both IT and compliance groups. Nevertheless, it is critical to get this right not only to create the right environment for directing automation across local scope and scale processes through the automation maturity curve, but also to ensure successful outcomes. Examples include improved evidence collection coverage and reduced time to prepare critical audit evidence. Automation can also be used to track performance, demonstrating better results than manual efforts. That said, with the enablers and challenges outlined above, we now turn to the future. The final section of the article presents strategic suggestions and emerging trends that support automated audit evidence harvesting, while also highlighting ServiceNow’s contribution to these efforts. However, despite the many projected benefits of automation, achieving fully automated audit evidence collection remains a significant challenge. The organizations will need to face technical, cultural, and regulatory challenges in addition to ensuring ServiceNow is implemented and configured effectively to realize its full potential. A procedure to think methodically about them in a way that understands the issues and forces may provide us with an idea of where they are likely to be encountered on the road, respectively, and how to deal with them. Table 1 below summarises some of the big challenges with corresponding frequent factors associated with success to address these challenges.

Table 1 Key Challenges and Success Factors in Automating IT Audit Evidence Collection through ServiceNow

Challenge	Description	Critical Success Factor
Data Quality in CMDB	Incomplete or inaccurate configuration items undermine audit reliability.	Strong discovery processes, regular reconciliation, and clear ownership.
Integration Complexity	Difficulties in linking ServiceNow with external systems and tools.	Phased integrations with standardized APIs and vendor-supported connectors.
Cultural Resistance	IT teams perceive compliance automation as burdensome or restrictive.	Transparent communication, role-based training, and seamless workflow design.
Evolving Regulatory Requirements	Frequent updates to laws and frameworks require system reconfiguration.	Agile compliance mapping and policy updates within ServiceNow modules.
Resource Constraints	Limited technical expertise or funding slows adoption.	Executive sponsorship and strategic investment in training and automation.

7. Strategic Recommendations and Future Directions

By using ServiceNow to automate IT audit evidence collection, we took a very meaningful step in risk, cost, and inefficiency mitigation. Nevertheless, the long-term success of these initiatives depends on approaches that address immediate compliance requirements, not only but also preparing organizations for anticipated changes in regulatory, technological, and operational landscapes. There are a variety of best practices to help enterprises sustain their automation capabilities and continue to grow.

One recommendation is that ongoing compliance be codified as part of an organisation's mission. The most important goal for automation is not to see it as a project to be implemented for a single audit or two, but as a long-term journey embedded in the governance structure of the enterprise. Subsequently, the identification of automation of audit evidence must be matched with maturity practices in corporate governance and then be integrated with compliance rates in enterprise performance dashboards. The fact that ServiceNow has the capacity to generate any type of role-based reporting makes ServiceNow a viable tool when it comes to integrating compliance in management reporting hierarchies [11]. The other direction of work is the development of interoperability between systems. An increased number of organizations are working in a hybrid cloud and multi-cloud environment with both 3rd party cloud applications and legacy back-end applications. Since ServiceNow is positioned as the single provider of audit evidence, its interoperability, enabled through standardized APIs, connectors, and integration structures, must be a priority in development [12].

The alternative strategic measure in prospect is also adaptive automation. The ever-changing nature of regulation requires automated evidence capture to remain flexible. Practices must be able to adjust to new compliance models or government policies without the need for a complete re-engineering process. One can go further by using the Artificial Intelligence and Machine Learning power of ServiceNow to detect anomalies and control failures and suggest prescriptive remediation procedures automatically [11-13]. One of the more forward-looking recommendations has been for a risk-based audit to be incorporated into automated audit systems. It is important to recognize that not every control or system requires the same level of monitoring and management. Evidence-gathering efforts should focus on assets that present the highest risk or those that are central to the most valuable business operations. ServiceNow risk management already supports risk scoring and association with configuration items. These capabilities will go beyond meeting compliance requirements and instead show how risks are actively driven by ensuring that audit evidence exists. Training and culture are a combination. No matter the platform that automates your technical process, to be successful, the process must be supported by personnel who understand the platform and also understand what the regulators expect of their processes. Organizations are encouraged to invest in ongoing relevant training programs that enable IT, audit, and compliance functions to set up, interpret, and act on automated evidence. Apart from technical training, cultural actions should reinforce the concept that compliance automation reduces the workload and supports the organizational resilience (not as a constraint) [15].

In addition to this, other aspects of good organization, such as scalability and sustainability, must be taken into consideration. Audit evidence automation processes must be able to scale as new business units, geographies, or compliance requirements exist in scope. Sustainability concepts should also be expanded beyond compliance, and, where appropriate, ESG metrics should be incorporated as part of an evidence framework. As ESG reporting grows in

importance, ServiceNow can serve as more than just a source of compliance case information within IT cases. It may also be leveraged as a repository for sustainability performance indicators [16]. From a research perspective, several interesting opportunities lie ahead. One is the use of blockchain to ensure deterministic immutability and strengthen audit trails. Another is peer-to-peer computation that translates regulatory requirements into actionable controls through natural language processing (NLP). In addition, predictive analytics can be applied to estimate compliance risks proactively, enabling forward-looking risk management. Our vision for the domain of academic/industrial interactivity described above will take a step closer to the theoretical and practical development of mature and rigorous models for automating auditing [17, 18]. Essentially, then, automation must be viewed by organizations as a process and not an endpoint strategically. This ongoing cycle of innovation and integration helps organizations to adapt to the shifting landscape of IT risk and compliance, yet it often falls short of keeping them consistently ahead in managing these challenges. Although ServiceNow provides the extensible platform and modular architecture to enable this, success ultimately depends on organizations aligning people, processes, and technology. Such alignment must be guided by a clearly defined 'North Star', the desired state of audit maturity.

8. Conclusion

In many respects, relying on manual processes to gather audit evidence has become obsolete. This is not only due to the growing complexities of the IT landscape but also because regulatory regimes are advancing their requirements for auditable evidence. ServiceNow Automation offers an effective solution by delivering efficiency, accuracy, cost reduction, and sustained compliance. Shifting from an audit-focused repository to purposeful value creation is essential, as unchecked compliance practices can impose significant burdens, often referred to as 'audit fatigue'. To avoid this, organizations must evolve beyond repetitive audit-driven practices and instead focus on making compliance value-adding to the everyday operations of ITSM. A three-tiered architecture comprising discovery, compliance mapping, controls enforcement, continuous monitoring, and automated reporting provides reliable audit data. This ensures that trustworthy information is available around the clock, 24/7. This should be feasible even as there will be data quality, integration complexity, cultural pushback issues, and executive sponsorship, with effective automation, training, and incremental implementation. Over time, the impacts become more evident. Companies that adopt interoperability, adaptive automation, risk-based auditing, and sustainability metrics will not only improve compliance but also build more resilient and robust digital ecosystems. ServiceNow plays a key role in realizing this vision by enabling enterprises to manage risk, control costs, and respond effectively to regulators and stakeholders in today's increasingly complex digital environment.

References

[1] Kummer, T. F., and Mendling, J. (2021). The effect of risk representation using colors and symbols in business process models on operational risk management performance. Journal of the Association for Information Systems, 22(3), 649-694.

[2] Lins, S., Thiebes, S., Schneider, S., and Sunyaev, A. (2015). What is really going on at your cloud service provider? Creating trustworthy certifications by continuous auditing. In 2015 48th Hawaii International Conference on System Sciences (pp. 5352-5361). IEEE.

[3] Henriques, J., Caldeira, F., Cruz, T., and Simões, P. (2024). A survey on forensics and compliance auditing for critical infrastructure protection. IEEE Access, 12, 2409-2444.

[4] Jayaraman, K. D. Composable Architectures For AI-Augmented Decision Support In Public Sector Systems.

[5] Azizi, M., Hakimi, M., Amiri, F., and Shahidzay, A. K. (2024). The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. Open Access Indonesia Journal of Social Sciences, 7(2), 1473-1482.

[6] Jayaraman, K. D. (2025). Federated Learning with Secure API Gateways for Enhancing Privacy in Distributed AI Systems.

[7] Chinthapatla, Y. (2024). Exploring the transformative benefits of integrating artificial intelligence into the configuration management database (CMDB). Journal Homepage: http://www.ijmra.us, 14(02).

[8] Jayaraman, K. D., and Kumar, L. (2025). Innovations in Web Application Security: Multifactor Authentication and Beyond.

[9] Chaqiqi, A., and Nugroho, A. (2021). Readiness analysis of data analytics audit implementation in Inspectorate General of the Ministry of Finance: An Indonesian case. The Indonesian Journal of Accounting Research, 24(2), 147-162.

[10] Friday, S. C., Lawal, C. I., Ayodeji, D. C., and Sobowale, A. (2024). Reviewing the effectiveness of digital audit tools in enhancing corporate transparency. International Journal of Advanced Multidisciplinary Research and Studies, 6(4), 1679-1689.

[11] Ali, O., Murray, P., Al-Ahmad, A., and Tahat, L. (2024). An integrated framework for addressing the challenges and strategies of technology adoption: a systematic review. Emerging Science Journal, 8(3), 1215-1242.

[12] Russo, A., and Lax, G. (2022). Using artificial intelligence for space challenges: A survey. Applied Sciences, 12(10), 5106.

[13] Jayaraman, K. D., and Jain, S. (2024). Leveraging Power BI for advanced business intelligence and reporting. International Journal for Research in Management and Pharmacy, 13(11), 21-36.

[14] Nawari, N. O., and Ravindran, S. (2019). Blockchain technology and BIM process: Review and potential applications. Journal of Information Technology in Construction, 24.

[15] Sayied, A. S., Batool, F., and Butt, R. M. (2025). Business Process Automation: Compliance Management. Journal of Business and Management Research, 4(2), 801-836.

[16] Dande, F., and Li, X. (2023). Enterprise Service Management Cybersecurity Threats: Exploring Cloud Configuration Management Database (CMDB) Implementation Within Community Colleges. 8th North American Conference on Industrial Engineering and Operations Management.

[17] Snow, P., Deery, B., Lu, J., Johnston, D., Kirby, P., Sprague, A. Y., and Byington, D. (2014). Business processes secured by immutable audit trails on the blockchain. Brave New Coin.

[18] Jayaraman, K. D., and Singh, P. (2024). AI-Powered Solutions for Enhancing .NET Core Application Performance. IJRAR-International Journal of Research and Analytical Reviews (IJRAR), 11(4), 71-84.

[19] Adekunle, B. I., Chukwuma-Eke, E. C., Balogun, E. D., and Ogunsola, K. O. (2023). Developing a digital operations dashboard for real-time financial compliance monitoring in multinational corporations. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), 728-746.

[20] Keller, A., and Subramanian, S. (2009). Best practices for deploying a CMDB in large-scale environments. In 2009 IFIP/IEEE International Symposium on Integrated Network Management (pp. 732-745). IEEE.