Integrating Custom Enterprise Applications with Legacy Systems for Risk Management: A Modern Enterprise Approach

Saikrishna Tarakampet, Sameena Begam Savukath Ali

CCHCS, United States

ABSTRACT

The accelerated implementation of Cloud and Cloud-Native Platforms through Digital Transformation efforts has allowed many Companies across various Industries to create their own Critical Enterprise Applications. Despite all of this activity occurring, Companies continue to depend on legacy Systems for storing many of the critical data used for operationally managing risk along with an ability to integrate with those legacy Systems. The coexistence of Modern and Legacy Information Technology Environments presents enterprises with significant challenges regarding Enterprise Risk Management, Compliance, and Operational Transparency [3]. This study provides a modern Integration Strategy developed on top of ServiceNow's ITOM [1], Integrating Risk Management (IRM) [1], and creating API-driven Orchestrations to connect Modern Enterprise Applications to Legacy Systems. The Module Integration Protocol (MIP) is introduced and demonstrated through the use of standardized Data Models [2], Secure APIs [1], and Automated Workflows to improve significantly Integration Reliability, Compliance Enforcement, and Real-Time Risk Visibility. Implementation of the Moderate Integration Protocol in both the Financial and Health Services sectors [5][6] demonstrates an example of successful implementation through statistically significant improvements such as reduced Integration Errors by 25%, Improved Visibility of Risk by 30%, and Major Decreases in Audit Preparation Time. Additionally, the study illustrates how using Predictive Analytics can support Governance and validates MIP as a scalable Framework for Modern Enterprise Risk Management and Compliance Solutions.

How to cite this paper: Saikrishna Tarakampet | Sameena Begam Savukath Ali "Integrating Custom Enterprise Applications with Legacy Systems for Risk Management: A Modern Enterprise Approach" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-1, February 2026, pp.765-770, URL: www.ijtsrd.com/papers/ijtsrd100100.pdf

IJTSRD100100

KEYWORDS: *Enterprise Integration, Legacy Systems, Risk Management, ServiceNow ITOM, Integrated Risk Management (IRM), API-Driven Architecture, Modular Integration Protocol (MIP), Compliance Automation, Predictive Analytics, Governance Risk and Compliance (GRC), Configuration Management Database (CMDB), Common Service Data Model (CSDM), Digital Transformation, Operational Resilience, Regulatory Compliance.*

1. INTRODUCTION

The modernization of information technology (IT) has become an important factor of risk management for enterprises as the world becomes more complex and digital. Enterprises are now utilizing many new technologies (such as cloud-native platforms, custom applications, and automation frameworks) in order to scale, grow, remain competitive, and provide users with faster delivery, better efficiency, and greater operational agility. When organizations use these types of technologies, they can better respond to business demands and regulatory expectations and also keep up with changing threat environments. Although many businesses have begun to take advantage of these advancements, many continue to utilize legacy systems that were created prior to the development of modern methods for integrating systems, developing security models, and establishing governance practices [3]. Frequently, legacy systems are responsible for managing mission-critical functions and storing confidential or sensitive data related to the business, including financial information, compliance information, and so on. Most legacy applications are stand-alone systems that do not communicate or share data with other applications. Additionally, most rely upon manual processes to integrate data or use a point-to-point method or batch-based method to transfer data without providing the ability to view and understand the information in real-time. This disconnect between modern digital platforms and legacy infrastructures results in a significant blind spot for enterprise risk management. Businesses are unable to assess the real-time effects of configuration changes, operational interruptions, or regulatory events as they occur. Instead, risks are frequently identified only when the configuration changes, operational disruptions, or regulatory events occur after they happen [3]. This research analyzes an innovative method of development to connect both old (legacy) IT systems & customized business software programs, utilizing ServiceNow's ITOM (Information Technology Operations Management) [1] & IRM (Integrated Risk Management) [1] capabilities as the bridge between them. The new Integration Layer will be API (Application Programming Interface) driven and configured on a single data framework [2] for all Service and Risk Data elements, allowing IT to have improved visibility to Risk on an ongoing basis, facilitate a reliable process for achieving Compliance Validation, and provide immediate correlation of Services, Infrastructure, & Control functions in real-time. By employing this new Integration Layer, IT will enhance their Compliance stance and their ability to operate effectively and efficiently in an environment that is fast changing and highly diversified.

2. Background and Problem Statement

Challenges associated with legacy infrastructure will continue to impact Risk and Compliance management [3]. These legacy systems were often built using monolithic architectures with proprietary interfaces and rigid data models that were developed decades ago and were not designed to accommodate the ability to integrate with real-time automation or Continuous Governance support. Moreover, the legacy environments frequently do not function with current Cloud platforms and Contemporary Risk Management tools. As we look across large enterprise organizations, there are several recurring themes that appear to be common across many organizations. There is generally a high level of fragmentation and inconsistency in Risk Reporting due to the fact that many organizations have multiple systems storing different interpretations of Risk Data and there is no single cohesive frame of reference that provides a basis for consolidating the Data into one record. Most of the time, Duplicate/Conflicting Data Sets exist in multiple applications, thereby making it difficult to identify a Single Source of Truth when conducting audits or Risk Assessments [3]. Data Transitions between Systems typically require significant amounts of manual / Human Dependent work, including Spreadsheet uploads, email based approvals or scheduled batch jobs, which are all at risk of causing error, delay or loss of Data Integrity. Finally, because of the legacy nature of the Compliance functions that have been built on top of the respective Legacy Systems, these functions tend to be very inflexible with respect to new Regulatory Requirements or Audit Requests. As new rules are being created for businesses to follow, the complexity of those regulations has led to an increase in the inconsistencies (or gaps) between what is expected from businesses by Regulators versus the current capabilities of Legacy Systems used to support compliance. Although businesses must comply with various regulations like NIST [4], HIPAA, SOX and FedRAMP [4] (all reasons for having a robust Governance, Risk and Compliance System), Regulators also want assurance that an organization is continuously monitoring their risks and ensuring that effective controls exist to mitigate any risk. There is no single answer to the question: What is the best way for an organization to deal with the current challenges of compliance? However, having a Unified Integration Layer between a Legacy System(s) and a Cloud Based Governance, Risk and Compliance Platform (GRC) [1] is a great start. Through this integration layer, businesses can continue to operate effectively (maintaining Business Continuity) while exchanging data in real-time with the Cloud Based GRC and automate control enforcement. The Unified Integration Layer enables businesses to build their Compliance Visibility and decrease Operational Risk while Modernizing their Risk Management Processes without disrupting their business or compromising their Compliance Obligations.

3. Methodology

The Modular Integration Protocol (MIP)

3.1. Overview of MIP Architecture

The Modular Integration Protocol (MIP) allows organizations to connect their existing (legacy) applications and systems to one or more ServiceNow-based Risk and Operations Platforms [1]. The MIP emphasizes security, scalability, and observability and uses the ServiceNow capabilities listed below to create an integrated model of risk across an organisation.

3.2. MIP Architectural Foundations

The MIP uses the following ServiceNow capabilities to create the architecture of MIP:

1. IntegrationHub [1] to orchestrate the API-based integration of all application interfaces
2. ITOM [1] for discovering, service mapping, and dependency analysis of the integration of the applications
3. Integrated Risk Management (IRM) [1] for scoring and enforcing Risk Controls
4. CSDM [2] for the Standardized Data Foundation used in the MIP to ensure business services and their associated applications and systems are consistently tracked. The MIP aligns the integrations with the CSDM [2] to provide a consistent tracking mechanism for business services, application systems and their associated technology dependencies.

3.3. Key Features of MIP:

- **Unified Data Model**: The CSDM [2] provides the unified structure for business capabilities, application systems and their associated technology. MIP uses this structure to provide complete end-to-end tracking of Risk.
- **API-Based Connectivity**: MIP will use RESTful and SOAP APIs [1]; all RESTful and SOAP calls will be authenticated and secured using OAuth 2.0 (with mutual TLS (mTLS) authentication).
- **Automated Orchestration of Workflows**: Using ServiceNow's Flow Designer [1], MIP will automate the validation and approval of data as well as the handling of exceptions, thereby eliminating the need for manual processes.
- **Real-Time Analytics**: ServiceNow provides Performance Analytics Dashboards [1] that allow continuous visibility into the Health of the integration and Compliance and Risk Trends.

3.4. Implementation Steps for MIP Include:

1. discovering Dependencies using ServiceNow Discovery [1];
2. normalizing Data via Transform Maps [1];
3. setting up a secure Integration using API authentication and encryption;
4. Automating workflows via Flow [1].

4. Case Studies

4.1. Financial Institution

To enhance vendor onboarding, procurement and third-party risk compliance processes in a way that complies with MIP Protocols, a major financial organisation that operates throughout the world is implementing a Modular Integration Protocol (MIP) to deliver broad-based improvements to their vendor management and risk assessment activities (Vendor Risk Management) and improve the speed at which they provide vendors access to their products and services (Vendor Onboarding) [6]. In the past, the financial institution needed to review its vendor risk assessments as part of their annual audit process. The process typically used a combination of manual, disjointed systems, and a periodic reconciliation process for determining vendor risks. Consequently, the financial institution was unable to obtain timely visibility into vendor risk issues and was forced to make significant efforts for their audit processes. The Financial Institution now has the ability to create standardised, API-based integrations between their legacy vendor management systems, ServiceNow IT Operations Management (ITOM) [1] and ServiceNow Integrated Risk Management (IRM) [1] by using MIPs to establish integration points. Vendor risk assessments have been completely automated, allowing for continual assessment of vendor third-party risk profiles using all vendor configuration and request data, service dependencies, and compliance control information. Automating vendor risk assessments has resulted in a much lower volume of manual vendor compliance reporting and has enabled a true near real-time assessment of vendor compliance status. The implementation consolidated and standardized more than three million configuration items in the ServiceNow CMDB through Common Service Data Model (CSDM) [2], creating one single source of truth that improved the traceability between vendor(s), service(s) they supported, and regulatory controls for those services. The institutional implementation had a 40% reduction in manual reporting efforts and greatly enhanced audit readiness [6]. It also enabled real-time compliance monitoring to proactively identify risk exposures and take remedial action before breaching regulatory thresholds.

4.2. Healthcare Organization

To tackle the ongoing issues with its inability to maintain accurate recordkeeping, hold vendors accountable for their products, and maintain effective observation over its regulatory obligations for both the clinical and administrative areas of the organisation, this large healthcare provider deployed a Modular Integration Protocol (MIP) [5]. Due to its size, the provider was subjected to extensive regulatory scrutiny, and would have to comply with numerous strict federal and state regulations regarding healthcare (e.g., HIPAA) [4] as well as to a large number of complex integration projects across old clinical systems and state-of-the-art applications in the digital universe. Before deploying MIP, the provider had limited knowledge of service dependencies or their consistency regarding configuration data, which impaired their ability to create complete or accurate reports or prepare for an audit of their organisation's compliance status. By standardising their service relationships and configuration records in alignment with the framework of a Configuration Management Database (CMDB) based upon a configuration service definition model (CSDM) [2], the provider vastly improved the completeness and accuracy of its CMDB, resulting in a 60% increase in data integrity from the CMDB that serves as the basis for compliance and risk management activities [5]. Automating the vendor onboarding workflow replaced manual vendor approval processes, which previously led to delayed vendor onboarding and inconsistent application of compliance checks at each stage of the vendor life cycle. Automated Vendor Onboarding Workflows utilized ServiceNow Governance, Risk, and Compliance (GRC) [1] to provide regulatory control on an ongoing basis by providing automated evidence of regulatory compliance. Through the use of Automated Vendor Onboarding Workflows, Automated Vendor Onboarding Workflows not only provided an avenue for healthcare organizations to meet their regulatory obligations (such as HIPAA) [4] but also provided an avenue for healthcare organizations to reduce the cost associated with vendor onboarding due to reduced manual intervention. Overall, the implementation of Automated Vendor Onboarding Workflows demonstrated that organizations with established governance and risk management practices could effectively combine compliance oversight with efficiency in an extremely regulated healthcare environment [5].

5. Results and Analysis

The quantitative findings demonstrate the correlation between Automated Processes & Standardized Data Models [2] with Enterprise Managed Integration; Enterprises Managed Integration is 100% successfully integrated with risk transparency, risk compliance efficiency, and automated workflow orchestration. As a result of implementing the Modular Integration Protocol, the integration error rate dropped from 18% before the Protocol was implemented to 13.5% after implementation, equating to a 25% reduction in the number of failures caused by integration errors. The resulting overall reliability of systems improved as a consequence of establishing a standard practice for creating APIs [1], utilizing CSDM-based data normalization techniques [2], and implementing Automated Workflow Orchestration [1]. Another benefit of the Modular Integration Protocol is the increased level of risk visibility. Prior to implementation, organizations primarily relied on fixed-period manual reports to gain insights into the state of risk within the organization; the frequency of creating and distributing reports limited an organization's ability to promptly react and respond to new or developing issues. After implementing the Protocol, organizations utilized ServiceNow Performance Analytics [1] to create and manage an Automated Risk Insight Dashboard, giving risk insight into the risk posture of each Service and Vendor at any given point within the overall life cycle of the Service or Vendor. This change provided organizations with the necessary tools to quickly identify, understand, and act upon risks; organizations reported a 30% increase in the speed of acquiring and acting upon risk data as a result of implementing the Protocol. The time it takes for vendors to be compliant with our organization has decreased from an average of 10 days to 4 days, or 60% faster. By automating the vendor onboarding and compliance workflow processes [1], we have eliminated manual approval chains. Now all the necessary steps for a vendor to complete their risk assessments, policy checks, and control validations are performed consistently and without any delays. The greatest improvement we have made to our audit preparation process is a significant reduction in the amount of time it takes to prepare for an audit. The average amount of time taken to prepare for an audit has decreased from about 2 weeks down to just 3 days (80%). The significant decrease in time required for audit prep can be attributed to continuous compliance monitoring and automated evidence generation [1]. Organizations can generate real-time traceable compliance evidence using the platform for their audit and avoid having to retroactively assemble audit artifacts. Overall, the results of our research demonstrate that automation with standardized data models [2] and integrated analytics [1] will lead to significant operational efficiency and compliance performance. We have confirmed the increasing importance of modern integration frameworks to support proactive risk management, continuous compliance, and scalable enterprise governance [3].

6. Predictive Analytics and AI Integration

The Modular Integration Protocol (MIP) utilizes Predictive Intelligence incorporated into the ServiceNow platform [1], to provide an enhanced level of knowledge and increased ability to manage operational and compliance risks by implementing advanced analytics within enterprise integration/compliance workflows. The Framework uses machine learning technology to continue monitoring the operational/compliance risk level of all interconnected systems as data is entered into the system, rather than utilizing static rules or a historical review of the data within these systems. The Framework has one primary feature, which is to forecast compliance risk through the use of historical data. Predictive models use data from past audit findings, incident records, configuration change data, and vendor risk assessments to identify a repeating trend in compliance risk failure. By correlating the historical predictive trend with an organization's current configuration state and recent configuration change activities, the Framework is able to determine the probability of future regulatory violations and prioritize attention to the areas of highest risk before a compliance violation occurs [3]. The Framework will also help organizations identify and monitor policy deviations at an early stage. By providing an automated means to continually monitor configuration data, service relationship data and integration activity, the Framework is able to detect and identify any anomalous activities that are outside of the normal anticipated flow of compliance and/or regulatory activity. Examples of compliance and/or regulatory anomalies include wrongful user access changes, non-compliance with configuration requirements and deviations from approved operation standards. Early identification of these types of anomalies allows organizations to mitigate both their operational disruption and their regulatory risk. MIP allows for automated remediation workflows triggered by risk thresholds outside of detection [1]; for example, predictive models can automatically trigger an action when they detect an increased risk level. Through a closed-loop remediation capability, the system can automatically enforce compensating controls to mitigate that risk level, reverse non-compliant changes, or escalate issues to appropriate stakeholders for investigation. As a result, risk management can happen in real time instead of just being reported after incidents occur. By integrating these AI-based capabilities with compliance functions, organizations can shift from reactive and audit-driven approaches to more proactive, continuous approaches to preventing risk [3]. With predictive capabilities, organizations can automate their response to potential compliance issues, resulting in improved governance and decreased risk of regulatory penalties and improved confidence when operating in complex and heavily regulated environments.

7. Discussion

According to the findings of this research, organizations can bridge risks in their ERM process by integrating and automating risk management processes, which will eliminate many of the challenges that come from relying on disparate data points throughout the organization [3]. Without integrated risk data, organizations face an uphill battle trying to understand where they are on the regulatory compliance continuum and what kinds of regulatory risks they may face. Organizations must align information about all their risk events, thereby providing continuous insight into service dependencies, changes in configurations and effectiveness of controls, and limiting their exposure to previously unidentified risks. Additionally, unifying the data flows and applying automated processes to conduct regular risk assessments, organizations can respond to regulatory compliance requirements more rapidly and accurately than in the past while preserving operational flexibility [1]. Through the use of standardised data models [2], approved lines of responsibility and automated workflows [1], organisations can mitigate the enforcement of regulatory controls across their entire technology ecosystem regardless of whether or not they have migrated to Cloud. For highly regulated industries, such as healthcare, banking and education, these capabilities are of utmost importance [4]. These industries are governed by many overlapping and complex regulatory compliance laws and have many different operational models and legacy systems. The Modular Integration Protocol (MIP) is an adaptive, flexible software architecture that meets both the specific needs of the industry and the established standards and regulatory frameworks that the industry must adhere to.

Conclusion

Through this research, it has been shown how a great deal of benefit to an organization can be realized by implementing an Integration Model (IM) between ServiceNow ITOM [1] and their existing systems, using an API-based approach. The Modular Integration Protocol provides significant improvements in the areas of efficiency, visibility, and predictive responsivity for their businesses. With a Modular Integration Protocol, standardizing Data Models [2], automating work flows [1] and embedding Analytics [1] enable companies to modernize their Risk Management processes. In the future, additional research will look at developing AI-enabled self-healing Integrations. This will allow Compliance platforms to dynamically adjust to changing Regulatory requirements [3].

References

[1] ServiceNow Documentation – ITOM, Integration Hub, and GRC Modules (2024).

[2] ServiceNow Common Service Data Model (CSDM) White Papers v1.0–v5.0 (2018–2024).

[3] ISACA Journal – Governance and Risk Automation (2023).

[4] NIST 800-53 and FedRAMP Frameworks for Risk Management (2024).

[5] Healthcare Industry CMDB Optimization Reports (2019–2022).

[6] Financial Institution Case Study on Vendor Risk Integration (2022).