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

Best practices for compliance and risk management in cloud-based procurement systems

Praveen Kumar Ilamurugan *

Pondicherry University, Puducherry, India.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(02), 028-034

Publication history: Received on 17 March 2026; revised on 04 May 2026; accepted on 06 May 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.2.0223

Abstract

As the trend of outsourcing procurement capacities of organizations to cloud-computing systems continues to rise, compliance management and risk management have found their way to the list of operational resilience. This paper will conduct a review of the best practices in complying with and managing risks in cloud-based procurement systems to synthesize the existing academic and industry literature findings. It addresses such basic points as secure system architecture, regulatory alignment, vendor risk management, data governance, and the role of analytics and automation to enhance compliance. Our attention is captured in the paper with the use of technologies like AI, machine learning, and ERP automation in industries like retailing, insurance, and healthcare to control regulatory compliance and respond to vendor disruptions in real time. Certainly, by implementing compliance-centric approaches and integrating risk management into the purchasing procedures, organizations can improve their security posture, audit preparedness, and strategic decision-making. The current paper offers a powerful guideline to align procurement strategies to contemporary regulatory and technological settings.

Keywords: Cloud Procurement; Compliance Management; Risk Mitigation; ERP Systems

1. Introduction

The relocation of the current procurement systems to cloud-based procurement systems is a radical shift in the way companies conduct sourcing, contracting, and supplier relations. Cloud technologies are scalable, offer real-time visibility of information, and are not expensive, but they expose organizations to a large spectrum of compliance and risk management problems. These include data sovereignty, regulatory compliance, third-party vendor risks, and technology vulnerability. Given that organizations are going digital in their procurement mechanisms, it is important to make sure that the systems used are secure, compliant, and resilient to keep the operations going and prevent sensitive information from being compromised.

The concept of compliance within the current enterprise ecosystem is being implemented and evolved as an active and fluid discipline applied to every facet of cloud-based procurement setups instead of a checklist process. Risk management, in its turn, is no longer limited to mere responsive controls, but has expanded to include improved analytics, predictive models, and AI-based surveillance. These developments are an indication of a radical change in organizational strategies, and the necessity to merge IT, legal, procurement, and risk functions into one compliance and security framework. This paper deals with the future of compliance and risk management in cloud-based procurement systems in regards to best practices, frameworks, and technologies.

* Corresponding author: Praveen Kumar Ilamurugan.

2. Security and Compliance Architecture in Cloud-Based Procurement Systems

The issues of security and compliance regarding cloud-based procurement platforms require an architectural solution that employs end-to-end visibility, encryption, and continuous auditing. Engineering systems should be in line with the compliance logic that is in line with industry specifications and international regulations. One of them is compliance with the provisions of ISO 27001, SOC 2, and GDPR, which provide guiding principles to organizations on how sensitive procurement information should be handled safely. The security models are transforming to identity-based models, including multi-factor authentication, role-based access control, and zero-trust architecture.

Cloud procurement systems are prone to data access control, third-party integrations, and vendor-related problems. Such systems are associated with numerous vendors and platforms that increase the attack surface. Stringent data protection policies like encryption at rest and in transit, and controls over access to data in third-party handling procedures, should be embraced. This is especially true in cases relating to insurance systems, in which different jurisdictions have various levels of compliance. Regulatory frameworks should be included in the cloud infrastructure and not addressed as a post-factum measure to provide continuity in compliance and make them legally defensible [1].

3. Risk-Based Procurement Strategy and Vendor Disruption Management

One of the most crucial aspects of cloud procurement systems is vendor-related risk management. The interruption of the supply chain, especially by suppliers, can be a catastrophe to organizational performance. The present procurement strategies, founded on risk-based approaches, use cloud platforms to enable flexibility in sourcing and predictive analytics. Under this strategy, risk scoring of vendors can be completed dynamically, and contracts can be re-allocated dynamically, while multi-sourcing protocols can be applied in order to avoid the risk of single-point failure.

Cloud-based procurement solutions are aiding the use of automated disruption notification and contingent planning, particularly in retail supply chains. Risk monitoring is achieved through high-tech dashboards that enable procurement teams to dynamically assess the reliability of vendors, compliance with contracts, and geopolitical risks. These systems enable flexible sourcing, which means that procurement teams can alter or negotiate with other suppliers in the event of disruptions, such that continuity is maintained. Through procurement intelligence being incorporated into cloud solutions, organizations gain the ability to maximize sourcing decisions and minimize risks in terms of finances, image, and regulatory compliance [2].

4. Compliance-First Cloud Migration Frameworks

The problem of compliance is important in other settings, such as finance and healthcare, in migrating to the cloud. Companies should use compliance-first cloud migration strategies to ensure that regulatory requirements are achieved without affecting agility. This includes ensuring that compliance lapses are checked before migration, using cloud service providers with strong security postures, and using automation tools to check compliance status in real time. The migration frameworks must cater to pre-migration audits, data classification, and legal assessments of data residency and sovereignty.

As the procurement environment presupposes the availability of transaction data, contracts, and supplier records, a breach of compliance may also result in legal action, fines, and loss of competitive advantage. The compliance-first model will ensure that these risks are mitigated through the application of procedural checks and regular monitoring. Besides, a shared responsibility model is required, according to which the responsibility for compliance between the cloud service provider and the procurement entity is shared. This segmentation helps offer transparency and faster reaction to incidents when compliance is violated [3].

5. Security and Resilience Metrics in Cloud Outsourcing

Since procurement systems are increasingly dependent on cloud infrastructure, security and resilience quantification becomes crucial. Organizations should also be equipped with a framework that will assist them in evaluating the effectiveness of their cloud systems against system attacks, data breaches, and system outages. The most important parameters that are used to indicate the resiliency of a cloud system are Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Mean Time to Detect (MTTD). These performance indicators can be specifically used in situations where procurement operations are in need of continuous interconnection for supplier onboarding, contract execution, and inventory control.

Cloud outsourcing is a notion that requires new risk measures to be redefined. For example, companies should verify the reliability of their cloud service provider, the strength of their Service Level Agreements (SLAs), and the process of data replication instead of merely ensuring that their data is secure in an internal data center. Procurement systems ought to be regularly subjected to penetration testing, threat modeling, and compliance assessment in order to ensure resilience. In order to track these metrics in real time, automated compliance and risk dashboards have become standard tools, enabling fast response and decision-making [4].

6. Data Governance in Cloud-Based ERP Procurement Systems

When dealing with compliance and security, effective data governance is important in cloud ERP systems that enable procurement functions. Cloud environments present problems of data duplication, inconsistency, and access control. Therefore, master data management (MDM), data lineage, and metadata tagging are all issues that should be addressed in data governance models. Procurement transactions tend to incorporate sensitive data in terms of both financial and operational matters that, once violated, can lead to grave legal and financial repercussions.

The governance processing of regulations in Oracle Cloud, as well as other ERP systems, enables the implementation of policies in real time and ensures audit readiness. A secure governance framework must consist of such measures as ensuring the principle of least privilege in governing data access and the possibility to register and audit all data operations. Moreover, procurement data privacy can be aligned with overall organizational policies by ensuring consistency and compliance across all departments and jurisdictions. This correspondence is of greater significance in multinational activities, whereby compliance with numerous local legislations is obligatory [5].

Table 1 Key Risk Areas and Corresponding Best Practices in Cloud-Based Procurement Systems

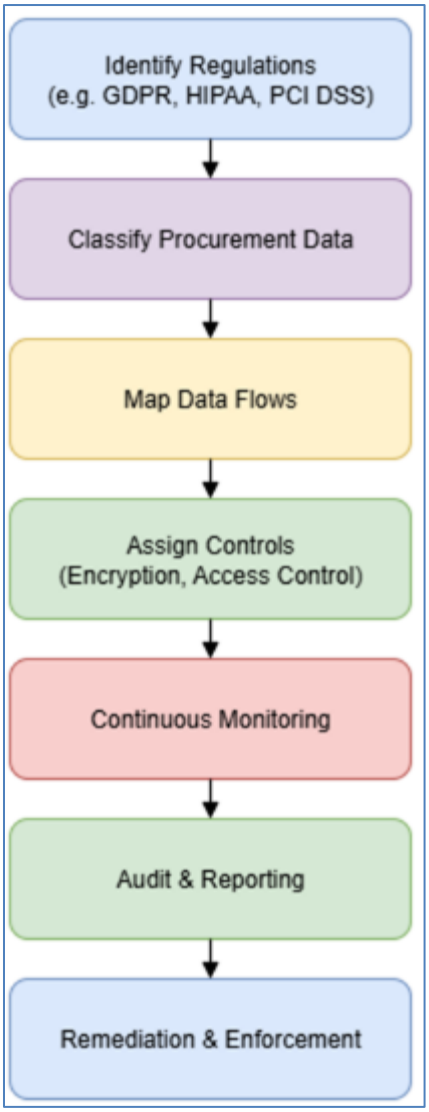
Risk Area	Best Practice
Vendor Disruption	Multi-sourcing, real-time risk scoring, contractual agility
Data Breaches	End-to-end encryption, zero-trust access controls
Compliance Violations	Pre-migration compliance audits, real-time monitoring
System Downtime	Resilience metrics (RTO, RPO), disaster recovery planning
Data Governance Failures	Metadata tagging, MDM integration, automated policy enforcement

Source: Compiled based on references [1] to [5]

7. Regulatory Challenges and Secure Cloud Deployment

Cloud procurement systems are struggling with a regulatory environment that is fraught with intricate and shifting demands. Organizations need to align their security designs to different legislations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS). In addition to stating what kind of data must be handled during procurement, these laws include provisions for reporting, breach notification, and user consent. Nonconformity may lead to severe penalties and reputational damage.

Implementation of cloud infrastructure in procurement should be well planned, whereby consideration should be taken in identifying where the data will be stored and the accessibility of the data. This entails the adoption of geo-fencing, data classification, and continuous compliance scanning. Companies must also develop internal compliance capabilities, since procurement officers, IT departments, and legal departments must collaborate. Secure cloud deployment must also be heavily controlled and patched, and the endpoints monitored to ensure procurement resources are not subjected to external or insider attacks [6].



Source: [6]

Figure 1 Regulatory Compliance Framework for Cloud-Based Procurement

8. Real-Time Analytics and AI in Risk Management

The delivery of cloud-based procurement systems with machine learning and real-time analytics is transforming the conventional paradigm of risk management. These technologies have also enabled predictive modeling to identify patterns and anomalies in procurement information, which enhances the forecasting of fraud, the assessment of vendor reliability, and the detection of supply chain disruptions. Using procurement departments as an example, real-time analytics allows various departments to monitor price variability, supplier lead time, and contract compliance, resulting in a holistic risk profile.

Machine learning algorithms are particularly valuable in the classification and prioritization of risks based on past and current information. AI models are adopted with the aim of taking into account the risks of insurers and claims history in cloud-based insurance procurement systems. This facilitates dynamic sourcing of contracts as well as strategic sourcing. AI-powered analytics is necessary because procurement systems are highly data-intensive, enabling them to display non-obvious correlations and emerging risks. In addition, automatic risk report generation is also essential for reducing human error and enabling faster decision-making [7].

These smart tools not only provide insights into operational activities but also make the process of compliance easier because they give warnings whenever transactions or vendor activities do not meet regulatory requirements. They also aid compliance officers in continuously monitoring procurement activities for red flags, ultimately making compliance

setups more agile and responsive. The more robust real-time data integration systems are built, the more procurement systems will rely on self-learning AI models that dynamically adjust risk parameters, creating a more adaptive and context-sensitive risk management environment.

9. Innovation in ERP Systems for Cloud Procurement

Some of the most significant developments have been cloud-based automation, artificial intelligence, and Oracle Integration Cloud (OIC), which have been made in an effort to improve procurement processes in Enterprise Resource Planning (ERP) systems. Existing ERP systems enable end-to-end automation of procurement processes, including request approvals, onboarding new suppliers, contract management, and invoice processing. The automation capacity makes sure that hands-on operational involvement is reduced, and compliance violations due to the human factor are minimized.

ERP systems (with embedded analytics and natural language processing (NLP)) are useful in making smarter procurement decisions. Automated systems can analyze vendor contracts, including clauses, to check regulatory compliance and detect inconsistencies. These capabilities are also becoming significant in manufacturing sectors that involve procurement across multi-level supply chains and regulatory controls. Cloud ERP also offers the facility for centralized control and standardization of operations across geographically distributed operations, ensuring that similar compliance protocols are adhered to.

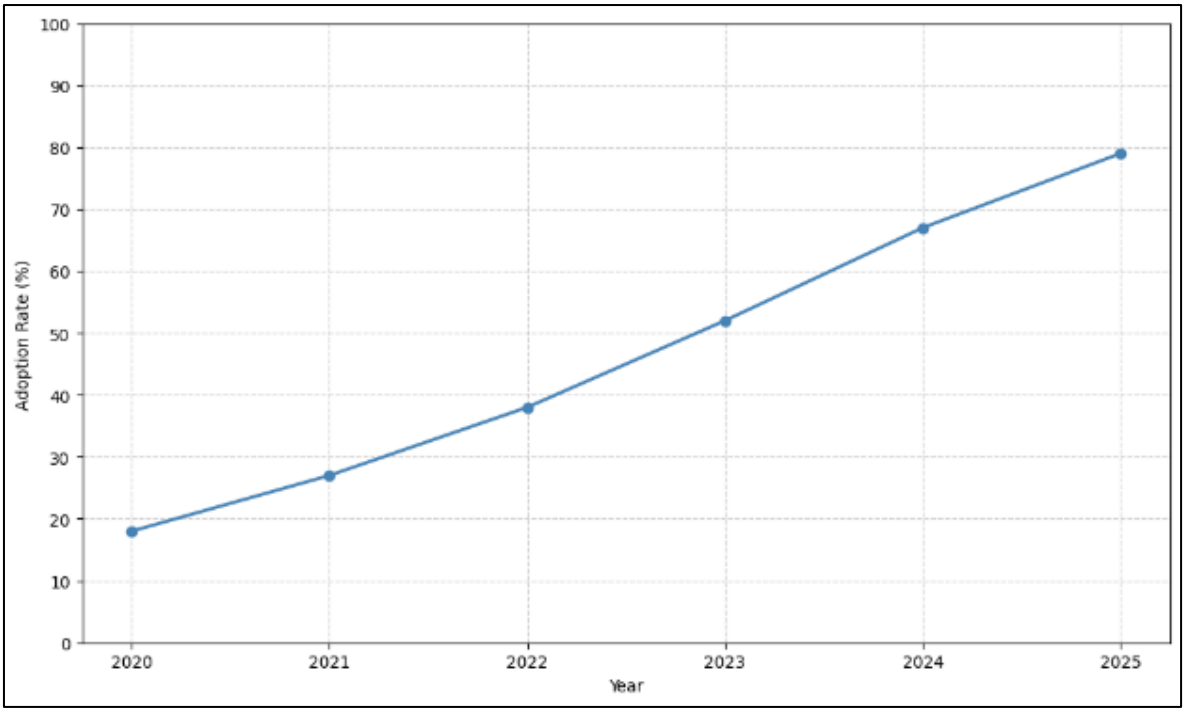
Besides, it is also coupled with Oracle Integration Cloud (OIC), which enhances the integration of procurement systems with third-party vendor systems and business applications. This compatibility assists in providing data consistency and audit trails. Artificial Intelligence also maximizes the potential of traditional ERP systems to provide predictive procurement recommendations based on vendor performance data and past purchasing behavior. Such sophistication is inclined toward a more proactive and compliant procurement environment [8].

10. Impact on SME Retail Models

Cloud-based enterprise systems are increasingly becoming a trend among SMEs operating in the retail sector in an effort to modernize their procurement systems and increase resilience. These systems are also priced lower and provide access to enterprise-level functionality such as vendor management, risk profiling, and spend analysis. Robotic compliance monitors and risk dashboards are practical for SMEs with no specific compliance departments.

Cloud procurement tools allow SMEs to grow their operations very fast without necessarily incurring a lot of expenses in the acquisition of capital, while facilitating compliance with regulations. The procurement system enables sourcing decisions to be highly responsive and agile due to the capability to access it anywhere. In addition, regulatory compliance is easily achievable within a multi-jurisdictional environment with the help of in-built compliance features, such as tax code validation, e-invoicing rules, and domestic data privacy settings.

Another advantage is that retail SMEs are experiencing improved business model performance due to the growing visibility of procurement and supplier collaboration tools. Procurement analytics can be used, for example, to choose the most effective suppliers, negotiate more favorable contract terms, and avoid delivery risks. This strategic action translates into improved inventory turnover, reduced procurement expenses, and more efficient operations. The transition to risk-sensitive and data-based procurement solutions has been driven by the implementation of cloud systems in SMEs [9].



Source: [9]

Figure 2 Adoption of Cloud-Based Procurement Systems in SMEs (2020–2025)

11. Role of Procurement Analytics in Risk and Resilience

The management of supplier risks has been anchored on procurement analytics. Evaluation of supplier performance, market trends, and compliance deviations using both structured and unstructured data will help organizations achieve resilience in procurement. These analytics tools are used on large amounts of procurement data to provide actionable insights on opportunities to reduce costs, improve contract compliance rates, and enhance vendor performance scores.

Supplier risk scoring is considered to be one of the most significant aspects of modern procurement analytics systems. By incorporating such variables as on-time delivery rates, past compliance incidents, financial stability, and geopolitical risks, organizations can rank suppliers in terms of reliability and exposure to risks. These insights are applied in the process of making decisions in day-to-day procurement activities and in long-term plans such as supplier diversification and contract renewal.

In addition, procurement analytics allows for the simulation of supply chain disruptions and the verification of organizational resilience. Most analytics platforms can perform scenario analysis, allowing procurement leaders to model the impact of specific risks such as currency fluctuations or supplier insolvency. This is vital in highly volatile markets, where procurement leaders must anticipate and react to sudden changes.

Regarding compliance, procurement analytics can be applied to create real-time dashboards and audit trail reports. These features ensure that procurement processes are tracked, traceable, and transparent to the level required for regulatory audits and internal governance [10].

12. Conclusion

Cloud-based procurement systems have revolutionized the landscape of compliance and risk management across all sectors. As procurement operations shift to the cloud, businesses must adopt security-first architecture, dynamic risk management tools, and adjust to regulatory shifts. The best practices discovered in this review are: transitioning to compliance-based migration models, the application of AI-based analytics, enhancement of ERP integration, and the application of data governance models that facilitate data integrity and regulatory compliance.

The combination of automation, real-time analytics, and scalable cloud infrastructure allows organizations to mitigate procurement risks proactively, ensure compliance, and enhance operational efficiency. These new procurement technologies not only enable cost savings but also support strategic resilience in an increasingly complex global market environment. As cloud technologies continue to improve, organizations must continue to refine their procurement strategies, integrating risk and compliance as integral components of the procurement system.

References

[1] Luca, C. (2025). Security, Compliance, and Risk Management in Cloud-Based Insurance Systems.

[2] Chowdhury, A. R. (2025). A systematic review of risk-based procurement strategies in retail supply chains: Sourcing flexibility and vendor disruption management. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 466-505.

[3] Owen, A., & James, L. (2025). Secure Cloud Migration Frameworks for Financial and Healthcare Institutions: A Compliance-First Approach.

[4] Risk, M., & Yasir, M. Measuring Security and Resilience in Cloud Outsourcing for Data-driven Risk Management.

[5] kumar Gali, V., & Vashishtha, S. Data Governance and Security in Oracle Cloud Ensuring Data Integrity Across ERP Systems.

[6] Bhardwaj, I., Devi, S., & Kumar, T. (2025). Securing the Cloud: Navigating Compliance and Regulatory Challenges. In *Risk-Based Approach to Secure Cloud Migration* (pp. 325-342). IGI Global Scientific Publishing.

[7] Sai, M. K. V. S. P. (2025). Integrating Machine Learning and Real-Time Analytics for Risk Management in Cloud-Based Insurance Platforms. *Journal of Computer Science and Technology Studies*, *7*(6), 533-539.

[8] Sola, S. R. Security and Innovation in ERP Systems Best Practices for AI, OIC, and Automation Integration.

[9] Bandara, H. A. D. J. M., & Oruthotaarachchi, C. R. (2025, February). Impact of Cloud-Based Enterprise Systems on Enhancing Business Model Performance in Retail SMEs. In *2025 5th International Conference on Advanced Research in Computing (ICARC)* (pp. 1-6). IEEE.

[10] Rashid, H. (2025). The Role of Procurement Analytics in Enhancing Supplier Risk Management and Resilience. *The International Journal of Business Quantitative Economics and Applied Management Research*, *8*(02).