International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P112
Eureka Vision Publication | Volume 3, Issue 4, 122-133, 2022

Original Article

Risk Monitoring & Mitigation Strategies for Oracle Cloud ERP Implementations: A Governance Framework for Risk Control

Vinay Kumar Gali[1], Bhargav Krishna Eruvuru[2]
[1,2]Independent Researcher, USA.

Abstract - Enterprise Resource Planning (ERP) is highly essential in the contemporary operations of an organization due to the end-to-end integration of business processes, additional development of data transparency, and strategic decision-making. Oracle Cloud ERP has been a significant solution in the market of modern-day ERP solutions because of its scalability, security, and cloud service. Nevertheless, the technicality of the cloud-based ERP implementations presents a substantial level of operational, technological, financial, and organizational risks. Poor risk management practices tend to cause project extension, over-run, breach of data security and poor performance of system. The paper will present a detailed governance system that can be used to monitor and control risks related to Oracle Cloud ERP implementation. The paper is a synthesis of the literature which is available on ERP risk management, cloud governance, and enterprise IT controls to determine significant risk categories and control mechanisms. An organized approach to risk identification, assessment, monitoring and mitigation is built up and justified by conceptual analysis and simulated case situations. The offered framework focuses on multi-layer regulation, ad hoc management, responsibility, and commitment among the stakeholders and alignment to organizational goals. The quantitative risk assessment models and qualitative control procedures are included to help in up-stream situations such as decision making. Findings indicate that the framework helps to increase the stability of implementation, compliance, and operational disruption. This study is important to the literature on ERP governance in that it provides a methodical and scalable way of addressing risk in the running of cloud-based enterprises. The results are likely to help healthcare practitioners, consultants, and policymakers to enhance the success of the Oracle Cloud ERP initiatives.

Keywords - Oracle Cloud ERP, Risk Management, IT Governance, Cloud Computing, Enterprise Systems, Risk Mitigation, Project Management, Information Systems Security.

1. Introduction

1.1. Background

Enterprise resource planning (ERP) systems are very vital in the contemporary organizations as it aligns the basic business operations like finance, human resources, supply chain, procurement, and customer relationship management in one information system that is centralized. With this integration, there is smooth exchange of data, heightened coordination, and better interdepartmental decision-making. Generally, the past organizations were using on-premise ERP solutions that involved massive capital investment in hardware, software license and dedicated IT infrastructure as well as ongoing maintenance and technical support. Acquisition of these systems also required a lot of internal expertise to handle upgrades, security and system performance. Due to the fast development of the cloud computing technologies, several organizations have migrated to cloud based ERP systems to eliminate these constraints. Cloud-based solutions are cost-effective, with subscription models, and are scalable to meet the emerging demand of the business, more flexible in their operation as they can be accessed remotely and deployed and implemented more quickly. Of all the existing cloud ERP environments, Oracle Cloud ERP has become one of the most popular solution offering modularly designed system, real-time analytics tools, and highly compliant features. Its highly modular format enables companies to install discrete functional units depending on the needs and integrated analytics facilitate systematic decision-making as well as monitoring of performance. Also, the internal compliance tools are designed to help companies comply with the regulatory and industry standards. The migration of the conventional systems to cloud-based ERP creates new technical, organizational and management complexities despite these benefits. The questions of data migration, system integration, reliance on vendor, security and change management usually bring serious problems at the implementation stage.

1.2. Importance of Mitigation Strategies for Oracle Cloud ERP Implementations

The successful deployment of Oracle Cloud ERP systems is not only "technological capabilities based" but also it is the capability of the organization to preempt, control, and mitigate the possible risks. Mitigation strategies are critical to making sure that the technical, operational and the organizational issues do not compromise the performance and business continuity of the system. Considering the business-wide nature and complexity of ERP systems, mitigation strategies with a high degree of organization are required to ensure the stabilization of the situation in the long term, ensuring a high level of security and value creation. The subsequent subsections underscore the pertinent aspects where mitigation plans make successful oracle cloud ERP implementations.

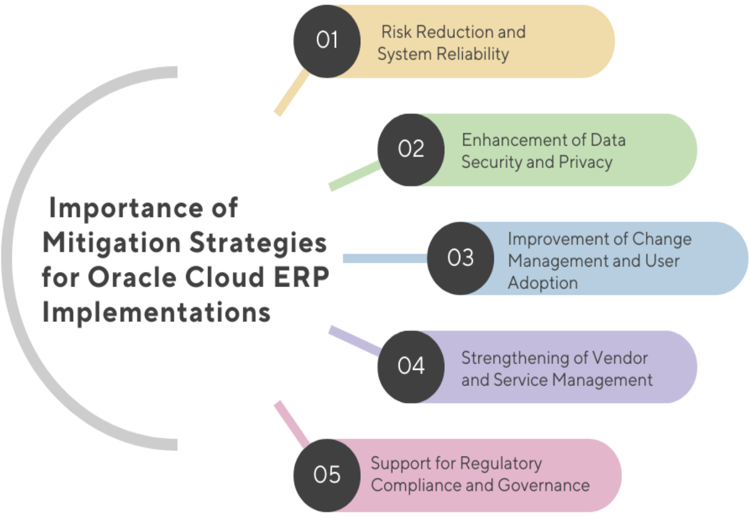
Importance of Mitigation Strategies for Oracle Cloud ERP Implementations
01
Risk Reduction and System Reliability
02
Enhancement of Data Security and Privacy
03
Improvement of Change Management and User Adoption
04
Strengthening of Vendor and Service Management
05
Support for Regulatory Compliance and Governance

Figure 1. Importance of Mitigation Strategies for Oracle Cloud ERP Implementations

1.2.1. Risk Reduction and System Reliability

The mitigation strategies aim at reducing the probability and effects of the risks associated with the system as one of their major objectives. Migration of data, system configuration and integration with third party are some of the complex procedures in the Oracle Cloud ERP implementation that are likely to suffer technical breakdown and disruption of operations. The effective mitigation efforts such as comprehensive testing, gradual implementation and backup procedures are useful in curbing the downtime of the system and continuity of business processes. Through effort to counter possible vulnerabilities, organizations are able to improve the reliability of their systems and steady delivery of their services.

1.2.2. Enhancement of Data Security and Privacy

Cloud-based ERP systems store and manipulate numerous sensitive organizational and customer data, hence they can be good targets of cyber threats. Security-related mitigation measures, including access controls, encryption, multi-factor authentication, and periodic security audits are required to defend the confidentiality and integrity of data. These measures are applicable in the context of Oracle Cloud ERP intending to make organizations meet the data protection requirements and minimizing the risk of the unwarranted access or data breaches. Enhanced security measures also create an element of trust amongst the stakeholders in the system.

1.2.3. Improvement of Change Management and User Adoption

Other common problems of ERP implementations include resistance to change and insufficient readiness by the users. It is possible to mitigate the shifts between the legacy systems and the Oracle Cloud ERP using mitigation strategies that involve stakeholder engagement, communication, and training. Awareness campaigns, user support and structured training programs help employees to work out the skills and confidence needed to use the system effectively. The increased user adoption will minimize the mistakes in operation and maximize the overall leverage of the system.

1.2.4. Strengthening of Vendor and Service Management

Oracle Cloud ERP implementations are based on vendor support and service-level agreements. The poor coordination between vendors may cause a lag in resolving issues, gaps in performance, and higher costs. The development of mitigation techniques that include: well negotiated contracts, performance audit, and frequent review meetings are effective in enhancing the relationship between vendor and providing quality services. These are meant to create transparency and accountability and, therefore, decrease the risks associated with dependency.

1.2.5. Support for Regulatory Compliance and Governance

Businesses that function within controlled settings need to make sure that their ERP software is within challenging regulations and business mandates. Compliance mitigation strategies on monitoring, documentation, and audit preparedness help organisations to comply well with the regulatory requirements. Compliance is another tool in the Oracle cloud erp that when implemented with internal governance policies assists in mitigating risks of lawsuits and improves accountability towards the company. Good administration systems with mitigation mechanisms also ease predictable policy implementation and ethical conduct of business.

1.3. A Governance Framework for Risk Control

A risk management system governance is an essential factor in the successful implementation and maintenance of the ORacle Cloud ERP systems. Considering the complexity and interdependence of the ERP environments, organizations need well-organized mechanisms to control the decision making, responsibilities, and system performance. A successful form of governance offers a form of formality, whereby the strategic objectives, operational mechanisms, and technical controls are synchronized so as to reduce risks and increase accountability of the organization. A well-defined role, policies, and procedures can make such a framework relevant in such a way that the risk management activities can be integrated into the normal business operations as opposed to being considered as isolated projects. The suggested governance system focuses on the multiply-layered approach integrating the strategic governance, operational management, technical protection, and compliance control. On a strategic level, the executive leadership sets the levels of risk tolerance, priorities of investments, and policies used to make ERP-related decisions. This makes the implementation of the system as well as its use to be kept in tandem with the organization objectives as well as long term sustainability. The standardized processes, performance controls and coordination systems at the operational level facilitate effective management of the systems and prompt resolution of the problems. These will minimize operational uncertainties and increase the reliability of the service. Technical controls constitute the other important part of the governance system in that risks associated with data security, system availability, and infrastructure integrity are dealt with. Such measures as access control, encryption, system audits, and vulnerability checks prevent any unauthorized access and system failures. Concurrently, compliance oversight is used to enforce compliance with regulatory requirements, contractual and internal policies. Persistent compliance oversight and documentation procedures enhance openness and minimize legal and reputational threats. The single most important strength in the governance structure is its focus on accountability and constant improvement. Having managers, IT staff members, and outside providers with distinct responsibilities, the structure will encourage a coordinated risk management approach and minimise the lack of clarity in the decision-making. The frequent performance reviews, risk analysis, feedback, and mechanisms can help organizations to change the practice of governance in response to the changing technological and regulatory climate. Naturally, the Oracle Cloud ERP implementation is a matter of risk management, yet the system of governance facilitates a systematic and proactive management of the uncertainties in such projects. It makes organizations more resolute, facilitates informed decisions, and makes sure that technological investments generate long-term business worth.

2. Literature Survey

2.1. ERP Implementation Risks

Implementation of Enterprise Resource Planning (ERP) is a multi-faceted organizational mechanism, which implies high levels of technological and managerial challenges. Somers and Nelson (2001) categorized the risks surrounding the implementation of ERP as technical, organizational, and strategic, and argued that in most instances, ERP implementation fails due to a set of factors which are interconnected. Markus et al. (2000) indicated yet another significance of connecting the business processes with the ERP systems and active involvement of stakeholders in the implementation lifecycle. The failure to analyze requirements may result in mismatch of the system with the organizational requirements, and lack of appropriate training may restrict the usage capabilities of the system by the users. The issue of data inconsistency is also a significant one, especially at the time of system migration and integration because it influences the precision of non-operationality and decision-making. There can also be poor liaison with the vendors thus delay, over-runs, and low performance of the system (which are more likely to lead to project failure).

2.2. Cloud Computing Risks

Cloud computing has disrupted the deployment and management of ERP system by providing a level of flexibility, scalability and low cost to an organization. Nevertheless, Armbrust et al. (2010) were able to determine a number of potential risks existing with regard to cloud environments such as the issue of data privacy, service availability as well as the reliance on cloud service providers. Subashini and Kavitha (2011) also highlighted that the security issues are another serious obstacle to applying the cloud. The vulnerability of multi-tenancy exposes infrastructures of sharing to possible data breaches, whereas the limited visibility also restricts the capability of organizations observing and regulating their IT resource. Data governance is even more difficult with compliance as different regions have different regulatory requirements. Moreover, interruptions in the processes of service and downtime of the system may be really crippling in the business process, which places significant emphasis on the importance of risk management and contingency planning in cloud ERP systems.

2.3. IT Governance Models

IT governance models, including COBIT, ITIL, and ISO/IEC 27001 offer organized principles on how IT resources should be managed with appropriate regulatory compliance and alignment of IT strategies to organizational goals. The best practices involving risk management, service delivery, and information security are defined using these models. Weill and Ross (2004) noted that proper decision rights and accountability mechanisms have to be defined to attain effective IT governance. These structures promote transparency and organizational controls by providing formal roles and duties as well as performance measurements. Nevertheless, even though they are widely used, these modes of governance are mostly generic and they might fail to solve the unique issues that are related to cloud ERP systems. As a result, organizations have to tailor and adopt these frameworks and adopt them within their organizational technology and operational settings.

2.4. ERP Governance Frameworks

ERP governance frameworks are oriented to aligning the organization structures, leadership status, and management processes in order to achieve successful implementation and running of the system. Huang et al. (2004) suggested the governance models which are focused on strategic leadership, cross-functional cooperation, and the perfect communication between stakeholders. Likewise, Al-Mashari (2003) incorporated vital success factors like the support of the top management, maturity of project management and involvement of users as critical success factors in the ERP success. Such frameworks emphasize the significance of balancing between technical and business decisions and organizational culture. The good governance structures help in resolving conflicts, allocation of resources, and control of performances which lower implementation risks. However, most of the existing ERP governance models are mostly designed to support the conventional on-premise models and might not fully support the complexities that come with cloud-based models.

2.5. Research Gaps

Although there is a lot of research on ERP implementation, cloud computing threats and IT governance models, some gaps can still be identified in the literature. Majority of the studies do not have continuous risk monitoring mechanism that would help organizations to discover emerging threats proactively and respond to the resulting threats across the system lifecycle. Also, the focus on specific models of governance in cloud-based ERP system is low, and thus the lack of information to guide practitioners. A great number of studies are based either directly on quantitative or qualitative methods, and there is little incorporating both viewpoints integrated methodologies. Moreover, the strategies of alignment of vendor-client risks are not thoroughly explored, even though they are important in common clouds. The study aims to fill the gaps by coming up with an all-encompassing and reconfigurable governance model that incorporates the use of continuous risk monitoring, cloud-specific governance, and joint risk control activities.

3. Methodology

3.1. Research Design

The research uses a qualitative-quantitative hybrid research design by offering a comprehensive explanation of cloud-based ERP governance and risk management. The incorporation of qualitative and quantitative analysis into the research is important as it guarantees the balance of the approach that is inclined at embracing both theoretical and empirical-based perspectives. This liquidity research design increases reliability and validity of the conclusion as it gives an opportunity to compare the findings of various sources and to use several analysis methods.

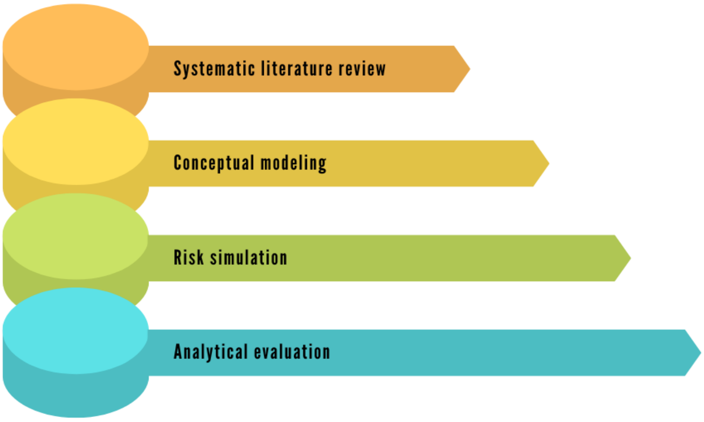

Figure 2. Research Design

3.1.1. Systematic Literature Review

A quantitative review of literature was carried out to find, discuss, and integrate already existing research on ERP implementation, risks when using cloud computing and IT governance models. Pertinent academic journals, conference papers, and within industry reports were studied based on the preset inclusion and exclusion criteria. Through this process, the high-quality and relevant studies have been selected and allowed building a solid theoretical basis and discovering gaps in the research area.

3.1.2. Conceptual Modeling

The theoretical framework of how the relationship between governance mechanisms, risk factor, and organizational performance under cloud-based ERP was developed was proposed by relying on conceptual modeling. On the lessons learned during the literature review, important variables and constructs were determined and designed into a combined model. It is a guiding model of data analysis and hypothesis development; it helps to conduct systematic research of the process of the risk governance.

3.1.3. Risk Simulation

The risk simulation was used to assess the risks, which are identified, and the effects they may cause on cloud ERP systems in various situations at work. The study is an evaluation of the impact of the change in risk factors on system quality through the probabilistic and scenario-based modeling methods to determine the effects on the system in terms of performance, security, and reliability. In this way, the possible failures can be predicted, and the proactive risk mitigation strategies can be developed.

3.1.4. Analytical Evaluation

To determine the effectiveness of the proposed scheme in governance and managing the risks, the analytical assessment was made. The quantitative data was subjected to statistical and comparative techniques, whereas the qualitative one was explained in terms of the thematic analysis. Combination of these analytical methods enables a full evaluation of the result of research and makes sure that the conclusions made are based on the empirical and theoretical arguments.

3.2. Risk Identification Process

Risk identification process was to be structured to systematically identify the threats that were likely to occur due to implementing cloud-based ERP and administering it. A multi method approach was embraced so as to cover extensively the technical, organizational and operational risks. The study also boosts the accuracy and completeness of risk factors identified because of the ability to incorporate various sources and perspectives of information.

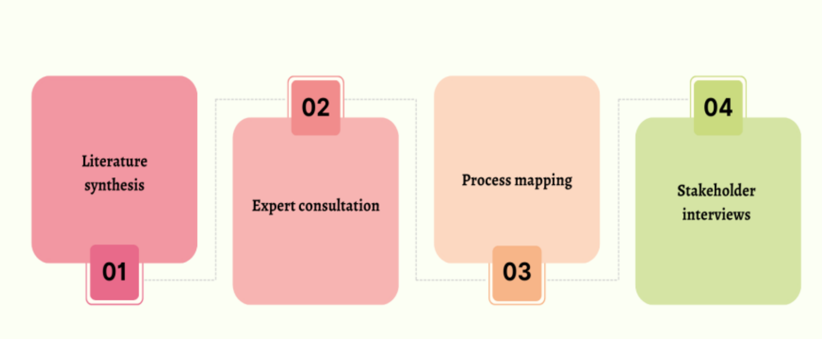

Figure 3. Risk Identification Process

3.2.1. Literature Synthesis

Literature synthesis was carried out in order to unify risk factors that have been mentioned in the past in regard to ERP systems, cloud computing, and IT governance. Reviewed peer-reviewed journal articles, conference papers and industry reports were compared in terms of recurring themes and risk frequently mentioned. This compilation allowed creating a preliminary risk inventory, which was a basis of further validation and enhancement.

3.2.2. Expert Consultation

Expert consultation was through contracting experts who had a lot of experience in ERP implementation, cloud services and information systems management. Those professionals were able to give some practical information on the issues of the real world and the emergent risks that are not well represented in the literature. These discussions and feedbacks were structured to ensure identification of risks are validated as well as to integrate the views of practitioners into the risk system.

3.2.3. Process Mapping

Organizational workflows and interaction of systems involved in cloud-based ERP operations were analyzed and modeled in process mapping. The main business processes, data flows, and decision points were graphically captured in order to determine the possible weak points and failures. This method assisted in the realization of risks at various phases of system implementation and utilization, hence promoting the mitigation which is specific to the risks.

3.2.4. Stakeholder Interviews

The interviews were executed as stakeholder interviews which described the managers, IT personnel, the end users, and external service providers participating in the ERP lifecycle. The experiences, concerns, and perceptions of the system risks among the participants were investigated using the employment of semi-structured interview protocols. The qualitative information gathered during those interviews gave a contextual information, and assisted in the revelation of undiscovered or underestimated risks, to a more complete assessment of risk.

3.3. Risk Assessment Model

The risk assessment model employed in the current study is going to be a quantitative risk evaluation model in that potential threats are evaluated in terms of a composite risk score (RS), which is the product of probability (P), impact (I), and difficulty of detection (D). The model uses a rational and methodological way of ranking risks that came along with cloud-based ERP systems. The model aids decision-makers in evaluating the probability of occurrence of the risk, but it also provides an understanding of the possible consequences of the risk and organizational capability in detecting it as soon as possible, since it incorporates various dimensions of risks. The multiplicative nature of the formula will guarantee that risks which have large values in any of the three constituents are duly highlighted hence averting the undermining of vital threats. Probability (P) can be understood to depict the potential of the occurrence of a given risk event over a certain time frame of operation. It is calculated using past information, professional experience and perceived system weakness. System complexity, frequency of previous incidents, and exposure to external threats are some of the factors that are put into consideration when giving the probability values. Impact (I) is the perceived supposed magnitude of the consequences in case the risk occurs, and they consist of financial loss, problems with operation, reputational losses, and legal or regulatory risk. The impact of any project is evaluated by the cost analysis, performance poll, and stakeholder feedback allowing the consideration of both tangible and intangible impacts of every project. Detection difficulty (D) is the level at which a risk can be discerned before it can inflict such material damage. This dimension indicates how well the monitoring tools, internal managerial controls and early warning systems are in place in the organization. Those risks that are not easily visible are usually detected too late and have more damage and hence should be prioritized. The difficulty in detection is checked in relation to transparency within the system, availability of real-time monitoring, and expertise of the personnel. The combination of these three dimensions helps to create a total risk score using the proposed model, which allows the identification of the identified risks and their comparison and ranking. The high-risk items will be prioritized in terms of prompt mitigation and allocation of resources based on high RS values. This organized way facilitates preventive risk management and enhances the practice of governance in cloud-based ERP settings because it can make informed choices and improve the performance constantly.

3.4. Governance Framework Design

The suggested governance framework has four layers with interconnecting relationships that will guarantee the effective oversight, control, and risk management of the cloud-based ERP systems. This multi-layered method is a means of facilitating the ability of organizations to achieve alignment of strategic goals with operational practices, technical protection and regulatory needs. Identifying the roles, responsibilities and control mechanisms at every level explicitly defines the roles and responsibilities of each level and encourages accountability, transparency and continuous improvement in the ERP governance process.

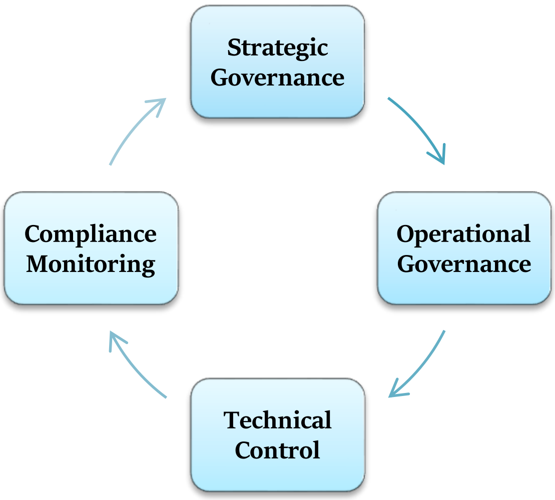

Figure 4. Governance Framework Design

3.4.1. Strategic Governance

The strategic governance concentrates on the long-term objectives of the organization, business approach and risk tolerance in the cloud-based ERP undertakings. It also includes the use of the top management and executive leadership in laying down policies, investment priorities and performance indicators of the ERP systems. This level makes sure that organizational objectives drive the key decision making processes in adoption of the systems, choice of vendors, and allocation of resources. Strategic governance can also formulate oversight committees and governance boards to review progress and conduct risk assessment of strategies hence advocate sustainable and value-based system implementation.

3.4.2. Operational Governance

Operational governance provides solutions to strategic goals and objectives in terms of actual processes and operations carried out in the day to day running of the organizations. It focuses on standardization of processes, role definition and coordination between the departments which are part of ERP operations. This layer is used to make sure that both system usage, maintenance and support activities are performed efficiently and consistently. Other activities related to operational governance include performance monitoring, incident management and service-level management which are used to ensure the system reliability and responsiveness and reduce operational risk to minimal.

3.4.3. Technical Control

Technical control revolves around the use of it and maintenance of technological mechanisms that can protect the cloud-based ERP system. The layer consists of access control, and data encryption, systems configuration, and backup process and network security controls. Organizations can minimize these vulnerabilities, avoiding unauthorized access or data breaches through the set of technical standards and security policies. Technical control entails periodic system audit, vulnerability examination in the system, and patch utilization to keep the ERP system safe and efficient against any emerging cyber threats.

3.4.4. Compliance Monitoring

Compliance monitoring makes sure that operations of cloud-based ERP are in accordance with the internal policies, industry standards, and legislative requirements. This layer deals with the ongoing evaluation of legal, contractual and ethical requirements in regard to data protection, privacy and information security. There is also the regular compliance inspection, reporting and documentation practices to prove accountability and transparency. Through the systematic adherence to vice, the organizations may reduce negative legal risks, prevent penalties, and preserve trust along with sponsoring responsible and sustainable governance.

3.5. Risk Monitoring Mechanism

The risk monitoring process is developed to ensure uninterrupted control of cloud-based ERP system in the form of frequently stated key performance indicators (KPIs). These indicators can help organizations quantify the performance of the system, the efficiency of operation and actual compliance status in real time. Keep the KPI trends that are easily visible to the management, monitoring, and analysis of these trends will help the management to develop a new risk, measure the performance of the prevailing or implemented controls, and to take timely corrective measures. This methodological form of monitoring assists in risk proactive control and improves the overall governance system.

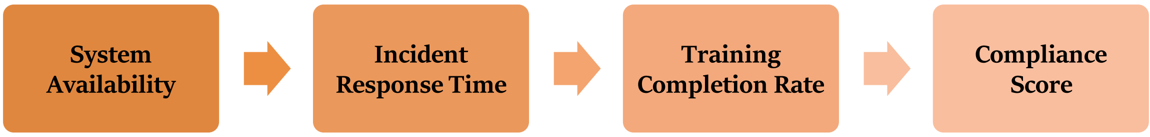

Figure 5. Risk Monitoring Mechanism

3.5.1. System Availability

System availability deals with the availability of cloud-based ERP system as being available and functioning its users at the appropriate times based on the production hours of the business. High availability plays a key role in having continuous business processes and organizational productivity. It is a KPI that is usually measured in percentage of uptime of a given time and is actively tracked within automated system logs and performance dashboards. Constant system downtime or loss of service could be a sign of infrastructure fragility, lack of support skills by the vendor, or resource constraints therefore indicated that it is time to make technical advancements or even rework the contract.

3.5.2. Incident Response Time

Incident response time is the time taken to identify, analyze and fix issues associated with the system which might entail security breach, performance failure and service disruption. This KPI is an index evaluating the performance of the incident management and support procedures within the organization. Reduced response time means that the IT teams are well coordinated, there are effective monitoring tools and they have clearly established escalation procedures. On the other hand, the longer the reaction time, the higher the lack of proper preparation in terms of expenditures and the decline of the reputation, which evidences the lack of resources.

3.5.3. Training Completion Rate

Training completion rate is a measure of how many of salespeople have gone through prescribed ERP and security training programs and finished them successfully. The indicator shows the dedication of the organization in achieving user competence and minimizing the human-related risks. Provided that employees are well trained they will be more inclined to adhere to system procedures and to adhere to security policies and make effective use of ERP functionalities. Lack of finishing training will lead to operational mistakes, system susceptibility, and system resistance adoption, and the importance of improving learning efforts.

3.5.4. Compliance Score

Compliance score assesses the level of adherence of the organization to internal policies and regulations and contractual requirements of cloud-based ERP activities. This KPI is based on the regular audit, self-evaluation and evaluation of third parties. A high score in compliance will mean that there is good governance, good control mechanisms and minimal regulatory risk. In their turn, the decreased compliance rates can subject the organization to both the lawsuits and negative publicity, which leads to the need to monitor the adherence rates and take the necessary measures to address the issue.

3.6. Mitigation Strategy Development

The systematic application of a control matrix that links the identified risks to relevant preventive, detective, and corrective controls was used as a method of developing mitigation strategy in this study. This procedural methodology is warranted such that any major risk that comes up in relation to the use of cloud-based ERP systems is dealt with using well-articulated administrative and technical solutions. The control matrix is an overall planning and monitoring tool that empowers organizations to think through visualizing the connections between risk factors, the governance mechanisms, and mitigation in line of action. The matrix can promote uniformity, responsibility, and transparency of risk management practices through the organization of risks and controls in a single framework. Its development started with the sorting of risks according to their risk scores, the rate of severity, and functional areas, including security, the operations, compliance, and vendor management. Stronger and multiple layers of controls were assigned to high-priority risks, whereas moderate and low-level risks were mitigated with respect to their degree. Access controls, policy enforcement and employee training programs which were preventive controls were aimed at minimizing the chances of occurrence of risks.

To ensure that the abnormal activities were identified in time, systems monitoring tools, audit trails, and intrusion detection systems were put in place. Those are the corrective controls such as incident response plans, data recovery procedures and system reconfiguration protocols that were developed to reduce the effect of the realized risks. Roles and responsibilities of each mitigation measure are also integrated in the control matrix, thus improving the governance and coordination by the stakeholders. The implementation, monitoring, and evaluation of controls are allocated particular duties to the management personnel, the IT staff, the vendors, and compliance officers. Such role system eliminates ambiguity and encourages successful coordination among the diverse organizational units. Moreover, specific performance indicators are also associated with every control to make continuous review and enhancement. Systematic mapping of mitigation strategies against risks helps organizations to redistribute their resources efficiently and focus on vital interventions by the proposed approach. The control matrix is dynamic and thus can be updated regularly in accordance with the fluctuating technological conditions, regulatory needs, and business goals. Consequently, this mitigation tool facilitates proactive risk handling, improved system resilience and increased the sustainability of cloud-based ERP management in the long run.

4. Results and Discussion

4.1. Framework Evaluation

The suggested governance structure was tested on the basis of simulated ERP implementation scenarios that are aimed at simulating the real organizational setting and operational difficulties. The effectiveness of the framework is evaluated by using these simulations which included technical, managerial, and environmental variables to determine the effectiveness of the framework in minimizing the risks and enhancing the system performance. The implementation of the proposed framework brought about the costs, security management, and project success outcomes, and by comparing the pre- and post-implementation system results, the study could measure the practical effects of the proposed framework implementation. The outcomes of the evaluation indicate a significant progress on the major parameters of key performance with the contribution of the framework to the increased governance and risk mitigation.

Table 1. Framework Evaluation

Parameter	Before Framework	After Framework
Failure Rate	42	18
Cost Overrun	35	12
Security Incidents	9	2

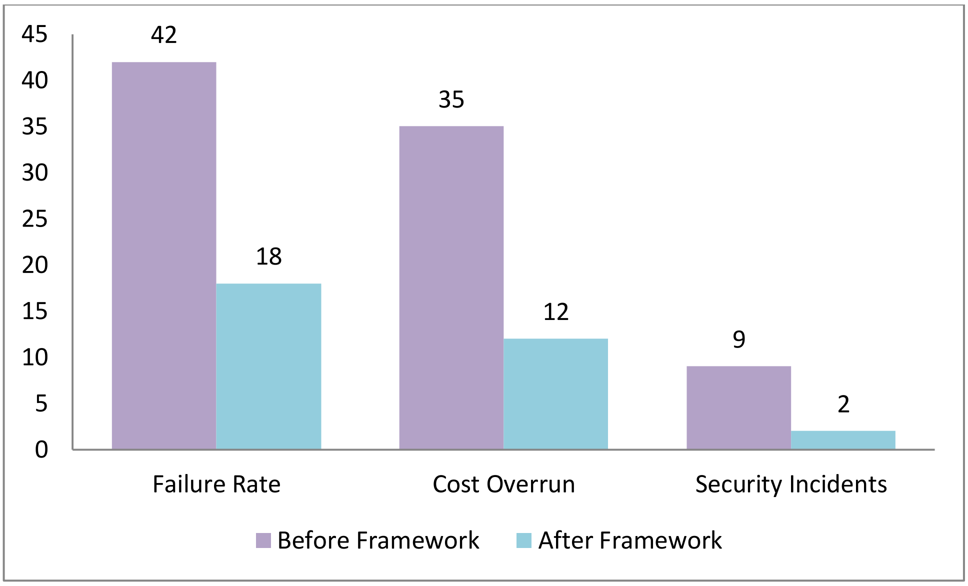

Figure 6. Graph Representing Framework Evaluation

4.1.1. Failure Rate

The failure rate is a percentage of the projects in the ERP implementation that failed to meet its targeted goals because of technical failures, managerial inefficiencies, or resistance on the part of the organization. Before the adoption of the proposed framework, the simulated scenarios experienced a high degree of failure rate of 42 percent implying a high level of vulnerability to the project. This was highly blamed on poor governance frameworks, poor risk monitoring and a poor coordination among the stake holders. The failure rate following the framework implementation rested at 18 percent due to an improvement in the strategic alignment, operations control, and more efficient decision-making processes. This cutoff indicates the capability of the framework to empower project planning, implementation and monitoring systems.

4.1.2. Cost Overrun

Cost overrun is used to mean how much the costs of the projects were higher than the original estimates of the cost of the project in the course of implementing ERP. Prior to the implementation of the framework, cost overruns were averaged at 35 percent which was primarily caused by unexpected technical problems, ineffective allocation of resources and constant changes in the system. Weak financial control and vendor weak management usually further complicated these challenges. The governance structure that was introduced resulted in a reduction in cost overruns to 12 percent, which means that the budget was better managed and financially responsible. This has been attributed to systematic evaluation of risk, organized procurement policy and performance monitoring that allowed highlighting the budget deviation early ensuring corrections were made.

4.1.3. Security Incidents

Unauthorized access, data breaches, system weaknesses, and other information security -related incidents threaten the integrity and confidentiality of the ERP systems. The pre-framework scenarios had reported nine large security incidents, which are indicative of a lack of technical control as well as lack of security awareness among users. These attacks were dangerous to information security and image. The results of the suggested framework implementation showed that the number of security incidents was reduced to two, which proved that the system security and risk preparedness had improved significantly. This was because access controls were enhanced, security audits were carried out on an ongoing basis, monitoring was enhanced and the user training programs were enhanced. All in all, the fact that security incidents have decreased is an indication of the effectiveness of the framework in enhancing the technical protection and advancing the information security culture.

4.2. Performance Analysis

Based on the conducted performance analysis, it works out that the suggested model of the governance and risk management greatly contributed to the effectiveness and reliability of the cloud-based ERP implementations. By incorporating the element of strategic management, operational alignment, technical controls, and compliance audit, the model countered the major flaws of the traditional ways of managing ERP systems. The fact that the project delays have reduced by 45 percent is a big step towards an increase in planning accuracy, assigning resources, and coordination of the process. We can explain this by the fact that the framework has well-organized risk assessment processes, clearly laid roles, and unceasing performance monitoring systems. Early detection of the possible bottlenecks with the systematic escalation processes allowed the project teams to eliminate issues in time, and thus, reduced schedule deviations and enhanced the performance of the entire project.

Further, there was significant security incident reduction of 70 percent, and this shows how the reinforced technical and administrative security measures worked. Introduction of effective access management systems, real-time monitoring software, and frequency security audits also enhanced the capability of the organization to prevent, detect and respond to cyber threats. Furthermore, employee awareness and adherence to the best practice were enhanced through the systematic training of users and clearly defined policies on the security. All these steps decreased the human error, unauthorized access, and system misconfigurations vulnerabilities, and enhanced the overall security posture of cloud-based ERP systems. The suggested model has also led to the reduction of compliance violations by 60 percent, which suggests its efficiency in making sure that operational practices meet the criteria imposed by the rules and regulations as well as the organization. This was made possible by compliance monitoring in real time, internal auditing on a regular basis, and automated reporting systems that helped organizations to observe deviations early in time and take corrective measures early enough. Such an offensive strategy minimized the risks of penalties by the regulatory authorities, lawsuits, and negative publicity. Additionally, the culture of responsibility and ethical behavior was cultivated by integrating the compliance need into the daily operation processes of employees and managers. Altogether, the identified enhancements on the project delivery, security management and regulation compliance provide the practical significance of the suggested model. The framework improves organizational resiliency, effective operation of the system over the long run and long-term competitive advantage of cloud-based ERP implementations by creating a unifying governance framework and encouraging ongoing risk management.

4.3. Discussion

The results of the research project show that the combination of continued monitoring systems and coordinated governance systems is extremely important when it comes to the effectiveness of the cloud-based ERP management. Operational: Uninterrupted monitoring allowed organizations to monitor the performance, security status as well as compliance rates at any point in time therefore, making it easy to identify possible risks, as well as operational inefficiencies. This positive attitude minimized the risk of system failures and prevented the influence of the appearing threats. The framework by including monitoring tools in the strategic, operational and technical governance layers enabled the transfer of risk-related information through the management levels at all times to facilitate timely and informed decision making. The second factor that was effective in enhancing the success of the proposed framework was the alignment of governance, which promotes the congruency among organizational goals, operating methods, and technical controls. The creation of multi level accountability frameworks demystified the roles and responsibilities of the executives, managers, IT personnel, and external vendors. This transparency minimized overlaps and conflicts in the process of decisions and encouraged partnership in solving problems. A better coordination between the stakeholders was seen specifically in the incident management area, negotiations with the vendors, and the compliance reporting where the actions of the stakeholder have to stay coordinated in order to keep the system stable. The coordination of the governance systems at the different levels also aided in the development of a common view of the risk management priorities, thus contributing to the organizational concerns over the reliability and security of the systems. Moreover, the risk prioritization became much more accurate and objective with the adoption of a quantitative risk scoring model. The model allowed managers to better differentiate between high and low-criticality threats by systematically assessing risks according to their probability, impact and the difficulty of detection. This systematic process minimized the use of personal judgement and experience resulting in more uniform and clear risk evaluation results. It, therefore, resulted in the more efficient allocation of resources to high-risk areas, which improved the effectiveness of mitigation measures in general. All in all, the joint use of the frequent monitoring, alignment of the governance, and quantitative evaluation of risk, provided a powerful and solid risk management setting. The coherent means enhanced the operational performance and security results, but also enhanced organizational learning and adaptability. This is indicated in the findings that propose that complexities and uncertainties in cloud-based ERP systems necessitate such integrated manner of governance in dynamic business environment.

4.4. Limitations

This study is vulnerable to various limitations that need to be taken into consideration when explaining the results even though the suggested governance and risk management model had a positive impact. The fact that there are no real-time empirical case studies of live cloud-based ERP implementations is also one of the constraints. As much as the simulated scenarios may have resembled real organizational settings as far as it could be, it cannot be fully able to capture reality, the unpredictability, and contextual issues that may be prevailing in real settings. Organizational culture, employee behavior, managerial dynamics, and external market pressures might have an impact on system performance in a way which is hard to simulate away. Consequently, applicability of the framework can be understood differently in practice once applied in a real operation setting. The fact that the study has used simulated data to assess the effectiveness of the framework is another major weakness. Although the method of simulating the environment offers a more controlled and systematic way of testing the governance models, it is pegged on a priori assumptions and parameterization levels. Such assumptions can never be a true projection of what an organization operates under, especially when the technological and regulatory environment is changing very fast. Quality of input data and methods of modeling also determine the quality of simulation results. Therefore, the differences in risk frequency, the patterns of using the system, and the behavior of the users in actual organizations may result in the different performance results as they were noted in this study. In addition, the specifics of the industry also introduce a further restriction to the overall applicability of the results. Various businesses, including healthcare, finance, manufacturing, and government services, are regulated with different requirements, risk profile, and business priority. Such differences in context can influence the applicability and usefulness of the suggested framework to different sectors. As cases in point, strictly controlled industries in terms of data privacy might need a stronger compliance, whereas competitive industries might favor system agility and innovation. Thus, it is possible that the framework might need additional modification in order to meet sector-specific requirements. Considering these shortcomings, further studies on the application on the suggested model should concentrate on its validation by longitudinal case studies and cross-industry research. This would make the studies more robust and offer more on the practical applicability and adaptability of the framework.

5. Conclusion and Future Work

The study has provided a fully developed model of governance of risk monitoring and mitigation in the implementation of the Oracle cloud ERP system targeting the most crucial issues in the implementation criteria that are complex system, security vulnerability, and compliance with regulations. The proposed framework offers an integrated approach of risk management across the ERP lifecycle by taking into account quantitative risk assessment models, multi-layered structure of governance, and systematic control mechanisms. The results indicate that the framework increases the stability of implementation, minimizes operational conflagrations and improves the organizational resiliency. With constant tracking, and organized responsibility, organizations have greater capabilities of foreseeing perceived threats and reacting adequately to the, in any case, arising challenges. In addition, the research paper is useful in the current ERP governance literature as it presents a cloud-based view, thus filling the gaps associated with dynamic risk, shared service, and vendor dependencies. Considering the practical perspective, the suggested framework provides useful solutions to those organizations that wish to enhance their governance and risk management practices. Formal governance committees by organizations allow it to have strategic control and a coordinated approach to decision-making within functional units.

Automated monitoring tools allow viewing and proactively interfering in real-time with the performance of the system, the state of its security, and its compliance with established rules. Accountability and reliability in service is increased through better coordination of the vendors backed by effectively compiled service level arrangements and communication procedures. What is more, enhanced cybersecurity measures, such as access control, encryption, and periodic security audits, can be used to alleviate the threat and preserve sensitive company information. Collectively, these actions enhance the creation of a strong governance environment in which technological investments are balanced with the business goals and regulatory provisions. Even though this study has made contributions, there are also several research opportunities that can be undertaken in future. Case studies with practical examples of Oracle Cloud ERP implementations would be more insightful in the long term effectiveness and flexibility of the presented framework. These studies might look at the way of changes of the governance practice with time following organizational development, technological shifts, and changes in the regulation. The use of artificial intelligence and machine learning methods should also be studied in future studies to predict risk analysis. Artificial intelligence models can also provide greater warnings capacity by detecting dynamic patterns and emergent threats that will not be readily detected by conventional means. Moreover, comparative studies between the cloud ERP providers of different vendors would allow the researchers to determine how generalizable the framework is and those best practices on different platforms. Lastly, a sector-based customization of governance is also a notable domain that requires more exploration as the differences between industries in terms of risk exposure, compliance mandates, and operational priorities might require sector-specific approaches to governance. Following such research directions, researchers, and operators will be able to enhance and develop the offered framework even further, thus contributing to more robust, secure, and sustainable cloud-based ERP systems.

References

[1] Al-Mashari, M. (2003). Enterprise resource planning (ERP) systems: a research agenda. Industrial Management & Data Systems, 103(1), 22-27.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[3] DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. Journal of management information systems, 19(4), 9-30.

[4] Huang, S. M., Chang, I. C., Li, S. H., & Lin, M. T. (2004). Assessing risk in ERP projects: identify and prioritize the factors. Industrial management & data systems, 104(8), 681-688.

[5] Ifinedo, P. (2011). Examining the influences of external expertise and in-house computer/IT knowledge on ERP system success. Journal of Systems and Software, 84(12), 2065-2078.

[6] Laudon, K. C., & Laudon, J. P. (2004). Management information systems: Managing the digital firm. Pearson Educación.

[7] Markus, M. L., Tanis, C., & Van Fenema, P. C. (2000). Enterprise resource planning: multisite ERP implementations. Communications of the ACM, 43(4), 42-46.

[8] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[9] Somers, T. M., & Nelson, K. (2001, January). The impact of critical success factors across the stages of enterprise resource planning implementations. In Proceedings of the 34th annual Hawaii international conference on system sciences (pp. 10-pp). IEEE.

[10] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[11] Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.

[12] Willcocks, L., & Griffiths, C. (2010). The crucial role of middle management in outsourcing. MIS quarterly executive, 9(3).

[13] Zhang, Z., Lee, M. K., Huang, P., Zhang, L., & Huang, X. (2005). A framework of ERP systems implementation success in China: An empirical study. International journal of production economics, 98(1), 56-80.

[14] Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of innovation assimilation by firms in different countries: a technology diffusion perspective on e-business. Management science, 52(10), 1557-1576.

[15] King, N., & Khan, A. R. (2012). Governance, risk, and compliance handbook for Oracle applications. Packt Publishing Ltd.

[16] Gupta, M., & Kohli, A. (2006). Enterprise resource planning systems and its implications for operations function. Technovation, 26(5-6), 687-696.

[17] Talluri, S., Kull, T. J., Yildiz, H., & Yoon, J. (2013). Assessing the efficiency of risk mitigation strategies in supply chains. Journal of Business logistics, 34(4), 253-269.

[18] Purohit, G. N., Jaiswal, M. P., & Pandey, S. (2012). Challenges involved in implementation of ERP on demand solution: Cloud computing. International Journal of Computer Science Issues (IJCSI), 9(4), 481.

[19] Jagoda, K., & Samaranayake, P. (2017). An integrated framework for ERP system implementation. International Journal of Accounting & Information Management, 25(1), 91-109.

[20] Ke, W., & Wei, K. K. (2008). Organizational culture and leadership in ERP implementation. Decision support systems, 45(2), 208-218.

[21] Gali, V. K. (2021). Enhanced Financial Forecasting in Oracle Cloud EPM: Predictive Analytics for Performance Optimization. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 2(2), 83-91. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I2P109

[22] Gali, V. K. (2021). Predictive Forecasting and Strategic Approach in Oracle Fusion ERP: Intelligent Planning Models. International Journal of AI, BigData, Computational and Management Studies, 2(3), 82-92. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V2I3P110

[23] Gali, V. K. (2021). Cash Flow and Working Capital Optimization Using Oracle Fusion ERP/EPM Data. International Journal of Emerging Research in Engineering and Technology, 2(4), 80-89. https://doi.org/10.63282/3050-922X.IJERET-V2I4P109