

Secure Adoption of Cloud-Based ERP Systems in Saudi Enterprises: A Governance Framework for Vision 2030.

Abstract:

Cloud-based enterprise resource planning (ERP) is being seen more and more as an infrastructure for integrated, data-driven management rather than merely as a simple way of hosting on-premise ERP systems. For businesses in Saudi Arabia, the strategic advantages are obvious: cloud delivery can speed up the process of implementation, provide extended access to people working in different locations, enable scalable analytics, and lessen the need for locally maintained infrastructure. At the same time, taking on cloud solutions does mean transferring key areas of control to external platforms and raises a number of governance issues relating to data stewardship, identity management, integration, service continuity, dependence on the vendor, auditability, and the organisation's readiness. This review draws on peer-reviewed evidence published between 2020 and 2025 and presents a governance framework for the secure adoption of cloud ERP in Saudi enterprises in line with Vision 2030. Thirty studies with verified DOIs were analysed using structured thematic coding focusing on cloud ERP adoption, digital transformation, ERP implementation in Saudi Arabia and similar environments, cloud security, and enterprise resilience. The synthesis indicates that security cannot be divorced from architecture, vendor governance, business process ownership, or change management; secure adoption thus demands governance throughout the entire lifecycle and not just a single technical evaluation. The proposed framework includes six areas: strategic decision-making rights, architecture and integration, data governance, identity and security, vendor and resilience governance, and capability and value assurance. It also incorporates stage-gates that run from business case approval through to post-go-live optimisation. The framework presents cloud ERP security as an enterprise governance capability which can help to support digital transformation while maintaining accountability, operational resilience, and measurable business value.

1. Introduction

Enterprise resource planning systems bring together a range of functions—including finance, human resources, procurement, supply chain, projects, asset management, and others—around common data and standard operating procedures. Since digital transformation has moved from a stage of isolated digitization to one involving the continuous redesign of business models, processes, structures, and decision-making practices [1-6], the importance of these systems within an organisation has grown. Cloud delivery further advances this transformation by shifting the ERP capabilities from infrastructure that is owned by the organisation to platforms operated by the provider, which can then be set up, updated, scaled, and accessed from various locations. In the case of large enterprises that have more than one site, legal entity, project, or service operation, this approach is able to lessen the friction associated with infrastructure while at the same time improving accessibility and the speed with which changes can be made.

Although the shift to a cloud ERP system alters the way control is distributed, traditional ERP programs tend to centralize a large number of operational and security decisions within the organization. In the case of cloud arrangements, on the other hand, the responsibilities are shared among the customer, the platform provider, the implementation partner, the managed service provider, the network operators, and in some cases also with other software vendors. Research into cloud ERP consistently names security, dependence on vendors, compatibility, architecture, support from top management, regulatory conditions, skills, and organizational culture as important factors affecting adoption [7-18]. Because of legacy applications, customized processes, identity stores, reporting platforms, and cross-border operations having to operate alongside a standardised cloud core, large organizations encounter greater complexity [16]. As a result, a cloud ERP program can be technically successful but still suffer from weak governance if the issues of ownership, the evidence of assurance, the service obligations, and the exit arrangements are not clear.

This is particularly significant in Saudi Arabia, since empirical studies on ERP and cloud adoption in the country show the impact of leadership, IT capability, change management, project management, trust in cloud providers, service-level verification, user involvement, post-implementation support, and the organizational context [19-26]. The Saudi organisations are also

carrying out broader digitalisation initiatives in which integrated enterprise data, automation, resilience, and analytics are expected to help with institutional modernisation and economic diversification [30]. A governance model for cloud ERP should therefore link cybersecurity and privacy controls with strategic transformation, rather than regard them as a separate technical activity.

Although there are existing studies that offer useful insights into this issue they are still fragmented. Research on adoption usually looks at why organisations intend to adopt a cloud ERP, while implementation studies focus on the difficulties of the project and the security literature deals with threats and the technical measures to mitigate them [10-18,27-29]. The studies concerning ERP in Saudi Arabia place a strong emphasis on success factors, culture, user adoption, and sustainability after implementation [19-23], while those relating to cloud computing in Saudi Arabia highlight trust, security, and organisational readiness [24-26]. However, there is less focus on how these findings can be combined to form a single lifecycle governance framework that defines the decision rights, control evidence, accountability, and assurance gates throughout the entire process, from the initial business case to steady-state operation.

This review therefore seeks to summarize the most recent evidence and establish a governance framework that is appropriate to the particular context for the secure introduction of cloud-based ERP systems into Saudi companies. The analysis is guided by five objectives: first, to determine the value mechanisms which make cloud ERP strategically important for enterprise transformation; second, to categorize the main governance risks that are caused or exacerbated by the use of cloud ERP; third, to interpret the evidence from Saudi Arabia and from similar regions regarding adoption and implementation; fourth, to turn this evidence into lifecycle controls and the allocation of decision-making powers; and fifth, to identify areas for further research in order to assess the effectiveness of governance in practice. The paper makes a contribution by changing the focus of analysis from individual adoption factors to the coordinated governance system that is needed to turn the capabilities of cloud ERP into secure and resilient enterprise results.

90

91 2. Review Methodology

92

93 A structured approach to review design was employed in order to look at the evidence that was
94 published between 2020 and 2025. This method is based on the principles followed by recent
95 high-quality reviews, which involve setting out clear search criteria, applying explicit eligibility
96 rules, using thematic coding, carrying out a comparative analysis, and providing a contextual
97 interpretation, rather than depending on an unstructured narrative [2,3,17,18,30]. The period
98 chosen for the review was intended to include contemporary cloud ERP architectures, post-
99 pandemic adoption trends, current research into digital transformation, and recent evidence from
100 Saudi Arabia, while at the same time excluding the older literature on ERP success factors since
101 the infrastructure assumptions in that work may no longer be compatible with current cloud
102 operating models.

103

104 The search terms were grouped into four categories: cloud ERP and ERP implementation; cloud
105 computing and enterprise architecture; security, privacy, governance, resilience, and vendor
106 management; and Saudi Arabia, the Gulf region, emerging economies, or Vision 2030. To find
107 relevant journal and conference literature that had been peer-reviewed, combinations of these
108 terms were used in scholarly indexes, publisher databases, and DOI metadata. The resulting
109 collection includes thirty studies, the publications of which span from 2020 to 2025. Before
110 being included, each bibliographic entry was verified by referring to the DOI landing page or the
111 publisher's metadata. The two reference papers provided were also looked at with regard to the
112 structure of their review, the depth of their analysis, the way they addressed the Saudi context,
113 and their presentation style; although their substantive claims were not copied, the 2026 paper
114 was not part of the citation corpus since it is outside the specified date range.

115

116 A study could be included only if it dealt with at least one of the key areas relevant to secure
117 cloud ERP adoption—namely, ERP or cloud ERP adoption, digital transformation, enterprise

architecture, cloud security and privacy, organizational readiness, ERP implementation or post-implementation governance, enterprise resilience, or ERP or cloud adoption specific to Saudi Arabia. It was excluded from the study if it did not have a verifiable DOI, was outside the period 2020 to 2025, was entirely promotional, or had no significant relevance to enterprise governance. Since there is still a lack of direct research on cloud ERP in Saudi Arabia, the evidence from studies on Saudi ERPs, those on cloud adoption in Saudi Arabia, and similar cloud ERP studies from emerging markets was combined with caution and not regarded as coming from identical populations.

The analysis employed a coding matrix consisting of six governance areas which had been developed step by step based on the available evidence: strategy and decision-making rights; architecture and integration; data governance; identity, security, and privacy; vendor and resilience governance; and organizational capability and value assurance. The findings were examined across three different layers of evidence: the general literature on digital transformation, the literature concerning cloud ERP and cloud security, and studies that were specific to Saudi Arabia or relevant to the region. Rather than averaging out contradictory results, they were kept. For instance, security and regulatory factors are important in some adoption studies but not statistically significant in others [14,15]; these differences were seen as indicating that intentions regarding adoption and the adequacy of governance are separate issues. This synthesis led to the conceptual framework illustrated in Figures 1 and 2 as well as the control matrix in Table 2.

3. Cloud ERP as an Enterprise Transformation Architecture

Cloud ERP should be seen as an option within enterprise architecture rather than as a decision regarding the purchase of software. Research into digital transformation stresses that technology only generates value when there are corresponding changes to the organization's structures, processes, capabilities, and performance logic [1-6]. It is important to note that if an existing ERP system is moved to externally hosted infrastructure without redesigning the allocation of

147 decision-making powers or the associated processes, the strain on infrastructure can be reduced
148 even though the scattered data, excessive customisation, weak ownership, and manual controls
149 will remain unchanged. Only when a standardised digital core is employed does Cloud ERP
150 become a transformative initiative, because it then enables processes to be simplified, data to be
151 integrated, workflows to be automated, and a scalable platform for analytics and for continuous
152 improvement to be established.

153
154 The literature points out a number of possible value mechanisms. Cloud ERP can help to reduce
155 entry barriers, lower the need for local infrastructure and maintenance, improve access from a
156 distance, speed up updates, and provide elasticity [7,11-15]. More recent studies associate cloud
157 ERP with resilience by highlighting availability, distributed access, recovery capability,
158 modularity, and the ability to reconfigure services when operating conditions change [17,18].
159 These advantages are especially pertinent to companies which have operations in different parts
160 of the world since shared platforms can decrease information latency and enable common
161 controls throughout the various business units. Evidence from Saudi Arabia also shows that a
162 successful ERP implementation can lead to the unification of core processes, enhance reporting
163 and data quality, and improve managerial analysis [23].

164
165 The same architectural setup, however, leads to dependencies. Software updates are now more
166 and more controlled by the provider; any integration has to take the provider's interfaces and
167 release cycles into account; network connectivity becomes even more important; data can be
168 spread across the main systems, the integration platforms, the backups, the analytics services and
169 third parties; and extensive customisation may clash with the cloud model's emphasis on
170 standardisation [10,12,16-18]. Vendor lock-in is thus not just a commercial matter; it can limit
171 the range of possible architectural decisions, make it difficult to leave the environment, affect
172 data portability, hinder incident response, and reduce bargaining power [12,16]. Similarly,
173 scalability is only advantageous if cost governance, access control, and configuration
174 management stop uncontrolled consumption and the expansion of privileges.

Table 1 puts together the main themes relating to the evidence. In the various studies it is found that benefits and risks go hand in hand: greater accessibility makes it more important to have identity governance; faster configuration leads to a greater requirement for change control; provider-managed infrastructure increases the need for contractual assurance and monitoring; integrated data enhances analytical value but at the same time raises the consequences of poor data quality or excessive access. Governance has therefore to deal explicitly with these trade-offs rather than considering cloud ERP as inherently safer or inherently more risky than on-premise ERP.

Another key difference lies in the transition from managing ERP systems in a project-based manner to taking on a product-oriented approach to platform management. In the case of on-premise systems, the focus has generally been on implementation, stabilization, and carrying out periodic upgrade projects. With cloud ERP, there are frequent updates provided by the vendor and a more constant stream of decisions regarding configuration, integration, and new features. This results in a change to the governance process. When looking at release notes, they need to be checked in the light of business processes, controls, interfaces, and training requirements; regression testing should concentrate on the most important transaction paths; and unused features should not be activated merely because they are technically available. A product-owner model can aid in keeping a prioritized roadmap while at the same time maintaining architectural discipline. The literature concerning digital transformation backs up this idea of continuous adaptation, whereby organizational design and technology develop together rather than through separate technology projects [2,5,6]. In practice, the value of cloud ERP depends on an operating model that is able to cope with repeated changes without compromising financial controls, data quality, or service reliability.

Theme	Value mechanism	Recurrent exposure	Governance response	Refs.
Strategic value	Scalability, accessibility, lower local infrastructure burden, faster updates	Business case optimism; unclear ownership; benefits not realized	Executive sponsorship, measurable benefits, defined decision rights	[7,12-18]
Architecture & integration	Integrated processes, shared platform, extensibility	Legacy complexity, interface failure, network dependency, lock-in	Target architecture, interface ownership, dependency mapping, controlled extensions	[16-18]
Data	Unified master data, better reporting, analytics	Leakage, duplication, poor migration quality, uncontrolled downstream copies	Data ownership, classification, lineage, reconciliation, retention and masking	[19,23,27,28]
Identity & security	Central access model, standardized controls	Excess privilege, weak segregation, compromised identities, configuration abuse	Strong authentication, least privilege, segregation of duties, recertification, logging	[27-29]
Vendor &	Managed	Provider	Due diligence,	[12,18,

resilience	infrastructure, availability, recovery capability	dependence, SLA ambiguity, concentration risk, weak exit capability	measurable SLA, recovery tests, portability and exit plan	24,26]
People & operating model	Standardized work, automation, faster decision support	Resistance, skills gaps, shadow processes, post-go-live degradation	Role-based training, process ownership, support capability, value assurance	[14,15, 19-23]

4. Governance Risks in Secure Cloud ERP Adoption

The first problem in terms of governance is accountability. Although a cloud ERP system spreads out the various operational tasks, responsibility for achieving business results, complying with regulatory requirements, maintaining financial controls, and overseeing data remains with the organisation that is adopting the system. It is necessary to have a well-defined authority structure which clearly separates out responsibility for processes, data, platform administration, security assurance, vendor management, and risk acceptance. According to research into the Saudi ERP situation, sponsorship, leadership, IT capabilities, project management, change management, and stakeholder ownership are all identified as key factors in ensuring successful implementation [19-23]. When these roles are not clearly defined, technical controls can be in place even in the absence of an accountable person to check that they are working effectively.

Another challenge is that of architecture and integration. Cloud ERP systems almost always function together with other systems; they swap out identity data, bank files, payroll details, procurement messages, project records, customer data, operational telemetry, and management information with the other systems in use. Architectural risks therefore arise not only within the ERP platform but also at the interfaces between systems. Research carried out on large-enterprise

cloud ERP systems has shown that data security, privacy, network dependency, mobility, vendor lock-in, and scalability are closely related architectural issues [16]. Although microservice-based and managed-service approaches can enhance agility and resilience, they also lead to a greater number of service relationships and technical boundaries for which observability, version management, and co-ordinated incident response are required [17]. Governance must include an authoritative integration inventory, approved interface patterns, dependency mapping, and release-impact assessment.

The third challenge is data governance. ERP systems make use of authoritative records for accounting, payroll, purchasing, inventory, projects, and management reporting. Although cloud migration can enhance the availability of data it can at the same time increase replication throughout test environments, analytics tools, integration services, and backups. Security assessments of cloud computing continually point to data leakage, tampering, intrusion, confidentiality, integrity, and availability as major issues [27,28]. A secure cloud ERP programme therefore requires clear rules regarding data classification, ownership, retention, encryption, migration reconciliation, non-production masking, backup controls, and the ability to trace data flows. The appropriate question to ask is not merely where the data are stored, but who has the authority to create, copy, transform, export, restore and delete them during the entire service lifecycle.

The fourth issue is identity and access governance, which is typically the most immediate means of control. Since ERP privileges can be used to authorise payments, alter suppliers, create users, change payroll information, post journals, or approve procurement, cloud access also goes beyond the corporate network, making it essential to ensure identity within the security framework. As zero-trust research shows, it is important that a user's location on the network should not lead to automatic trust and that access decisions should always be restricted by verified identity, context, and the principle of least privilege [29]. In the case of ERP governance, this means making use of federated identity where appropriate, implementing strong authentication, carrying out role engineering, ensuring segregation of duties, applying controls over privileged access, carrying out periodic recertification, monitoring emergency access, and

establishing quick processes for joining, moving and leaving employees. Particular attention should be paid to configuration rights since cloud administrators are able to modify workflows and security settings without having to change the application code.

The fifth issue concerns the governance of vendors and services. Research carried out in Saudi Arabia on the adoption of cloud services indicates that trust in the providers is affected by their reputation and the credibility of the service-level verification [24]. Another study on community-cloud services in the Kingdom also finds that confidence, privacy, integrity and availability are factors which influence acceptance [26]. It therefore follows that trust should be turned into auditable evidence rather than being regarded as a subjective opinion. Contracts and operating procedures must specify service availability, incident notification, recovery objectives, support escalation, data return, deletion, subcontractor transparency, audit evidence, change notification, and exit assistance. A service-level agreement will only be of any use if the metrics are measurable, the reports are reviewed, exceptions lead to action, and material failures have clearly defined escalation procedures.

The sixth aspect is resilience. Although cloud ERP can enhance an organisation's readiness, response, and recovery through the use of redundant infrastructure, remote access, and standard operating procedures [18], it is possible for concentration risk to rise if a number of vital processes rely on a single platform, a single identity service, or a single network route. Business continuity plans must therefore include scenarios in which the ERP service, the integration layer, the identity provider, the connectivity, or a key third party is not available. Recovery tests should focus on verifying business processes rather than simply restoring the infrastructure. Manual workarounds, accumulated transaction backlogs, reconciliation processes, and the sequence of recovery all require designated owners and tested thresholds. Moreover, resilience governance demands that the boundary of the provider's responsibilities be understood so that assumptions regarding backups or disaster recovery do not take the place of verified configurations.

In the end, organizational change is a matter of security and governance rather than merely a communications issue. Research carried out in Saudi Arabia and in other developing market environments indicates that culture, the skills of employees, the support of top management, the involvement of users, training, and resistance all have an effect on ERP outcomes [14,15,19-23]. If workflows are not well understood, shadow processes may arise, credential sharing could occur, uncontrolled spreadsheets might be used, there could be a large number of access requests, and workarounds might be introduced all of which undermine the formal control environment. For secure adoption it is therefore necessary for process owners and users to know the reasons for the existence of controls, to understand how exceptions are managed, and to see how new responsibilities alter everyday work. Training should be tailored to the specific role and should be reinforced following go-live, when users face real transaction pressures and when the original project team starts to disband.

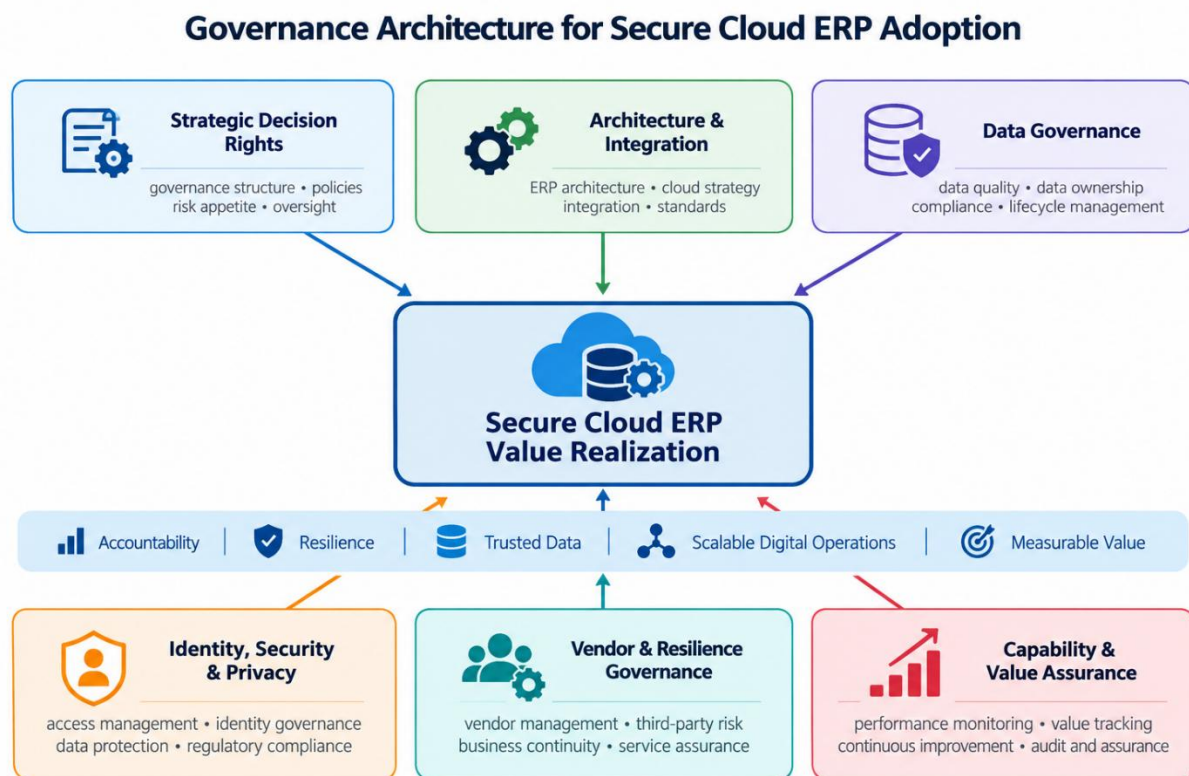


Figure 1. Integrated governance architecture for secure cloud ERP adoption in Saudi enterprises.

5. Saudi Context and Vision 2030 Alignment

The situation in Saudi Arabia provides support for the idea of integrated governance since digitalization of enterprises is taking place together with organizational growth, modernization, and rising expectations regarding data-driven management. Recent studies conducted in Saudi Arabia indicate that the value of an ERP system goes beyond simply installing the system; national ERP vendors consider sponsorship, leadership, IT capabilities, change management, and project management to be essential for the success of projects in the public sector [21]. Research into ERPs in the public sector emphasizes the importance of user involvement as well as wider organizational and environmental factors [19], and case studies carried out after implementation show that top-management support, training, testing, data migration, user adoption, employee retention, and ongoing support are still important following the technical deployment [20].

The evidence from the Saudi context brings a further aspect to the issue. Trust in the service providers and the presence of verifiable service level commitments affect acceptance of cloud services [24], and research in the healthcare sector shows that organizational decisions are the result of the interaction between technological, organizational and environmental factors [25]. Likewise, studies into the adoption of community cloud services place importance on confidence and on the protection of privacy, integrity and availability [26]. It therefore follows that a cloud ERP framework in Saudi Arabia should not suppose that a platform which complies technically will lead automatically to trusted adoption; it is necessary for governance to make the providers' commitments visible, to designate internal owners, and to produce evidence that executives, auditors, risk teams and operational managers can review.

Vision 2030 should be seen as the strategic framework rather than as a replacement for governance. Studies relating to Saudi Arabia's digital transformation link technological modernisation with competitiveness, resilience, and wider economic transformation [30]. Cloud ERP can help advance this objective by setting up standardised enterprise data, ensuring integrated workflows, offering scalable digital services, and improving management information.

Yet alignment must be shown through tangible results such as reduced cycle times, greater control effectiveness, higher service availability, better data quality, increased user adoption, greater cost transparency, and enhanced decision support. If Vision 2030 is treated merely as a rhetorical label without connecting the programme to operational outcomes, the business case will be weakened rather than strengthened.

The framework should also take into account the various types of enterprises in Saudi Arabia. For a government organisation, public accountability, auditability, and standardised service delivery may be the main concerns; for an industrial group, plant and project integration, the continuity of supply, and operational availability would be the priorities; and a diversified holding company would concentrate on the consolidation of multiple entities, the use of common master data, and the provision of shared services. Although these differences have an impact on how risk is managed, they do not affect the need for clear governance. The common requirement in all cases is that there should be traceability running from strategic objectives through to process design, platform configuration, control evidence, and operating metrics. This traceability helps to ensure that transformation programmes do not become mere assemblages of isolated technical initiatives and gives executives a defensible basis for explaining how investments in cloud ERP systems contribute to institutional performance.

6. Proposed Governance Framework

The governance architecture that is proposed is shown in Figure 1. At the centre of this architecture is cloud ERP value realisation, with six governance domains surrounding it which function as a mutually reinforcing system. The framework intentionally does not include cybersecurity within a separate perimeter; security relies on strategic ownership, architecture, data, vendors, resilience and user behaviour, while in turn these domains depend on security controls in order to remain trustworthy. The six domains should therefore be subject to common decision-making bodies, the sharing of evidence and the use of consistent risk thresholds.

355

356 The aspect of strategic decision-making determines the reason for the organization's move to a
357 cloud ERP system, specifies which processes should be included in the common digital core,
358 identifies which risks can be accepted, and clarifies who has the authority to approve exceptions.
359 The steering body should comprise the owners of business processes, finance, technology,
360 security, risk, data, internal control, procurement, and the major operating units. Its function is
361 not to handle the day-to-day configuration but rather to settle the cross-functional trade-offs. A
362 business case must set out the desired outcomes, the baseline measures, the scope of the
363 transformation, and the non-negotiable controls. This is in line with the evidence that leadership
364 and top-management support are consistent success factors for ERP projects both in Saudi Arabia
365 and in broader cloud ERP research [12,14,15,19-23].

366

367 The area known as architecture and integration governance is responsible for defining the desired
368 cloud ERP environment, the principles to be applied to interfaces, the strategy for extending the
369 system, and the limits regarding technical debt. Each interface must have an owner, possess a
370 data classification, use a specific authentication method, specify how it will behave in the event
371 of a failure, and include a monitoring requirement. Any customisation must be supported by a
372 justification which takes into account its effect on upgrades, security, and long-term
373 maintainability. This is especially important since the architecture of a cloud ERP system
374 involves dependencies relating to network access, platform releases, integration services, and the
375 provider's ecosystems [16,17]. Architecture governance should promote controlled extensibility
376 and avoid reproducing the complex legacy systems in the cloud.

377

378 The area of data governance gives ownership of key data items and sets up rules relating to
379 quality, migration, retention, reconciliation, access and subsequent reuse. Migration has to be
380 viewed as a kind of control transformation since duplicate records, inactive users, out-of-date
381 suppliers, inconsistent master data and historical access patterns should not just be copied over
382 into the new environment. The data owners must approve the cleansing rules and the
383 reconciliation tolerances, while the technical teams are responsible for documenting the lineage

384 from source to target. Once the system goes live, the data quality indicators should cease to be
385 checks that apply only to the project and instead become operational metrics.

386
387 Risk is turned into enforceable controls on the platform in the area of identity, security, and
388 privacy. The basic requirements are strong authentication, the principle of least privilege,
389 segregation of duties, governance of privileged access, logging and alerting, the management of
390 vulnerabilities and configurations, secure integration, encryption, and regular reviews of access.
391 These controls must be based on risk: the privileges involved in making payments, processing
392 payroll, accessing supplier master data, carrying out financial postings, or carrying out security
393 administration should have stronger preventive and detective safeguards than those needed for
394 ordinary inquiry access. The control model must also take into consideration the non-human
395 identities used by integrations and automation. As shown in the cloud security literature,
396 confidentiality, integrity, and availability should be protected by a layered approach rather than
397 by relying on a single defensive mechanism [27-29].

398
399 The fifth area, which is vendor and resilience governance, turns external dependencies into
400 managed responsibilities. When carrying out due diligence, one should look at the service
401 architecture, the operational history, the assurance reports, the arrangements with subcontractors,
402 the recovery capabilities, the security responsibilities, the support model, the possibilities for
403 data portability, and the exit options. The contractual commitments have to be put into practice
404 by means of monitoring. Even if a migration is not planned for, the organisation should still keep
405 an exit plan since a credible exit capability ensures that data portability, documentation, and
406 dependency management are properly handled. Resilience testing should involve scenarios in
407 which the system operates in a degraded mode as well as coordinated exercises that bring
408 together business teams, not just tests concerning technology recovery. Research that has linked
409 cloud ERP to enterprise resilience indicates that readiness, response, and recovery are separate
410 capabilities that need to be deliberately managed [18].

The sixth area, capability and value assurance, guarantees that governance will last beyond the implementation stage. Essential elements include role-based training, process ownership, internal support capability, vendor knowledge transfer, the use of performance metrics, and a review following go-live. Evidence from the Saudi case shows that support, training, adoption, retention, data migration and testing still have an impact on the sustainability of the ERP system after it has been deployed [20]. Value assurance must therefore compare the benefits that have actually been achieved with those stated in the approved business case and at the same time monitor any unintended consequences, such as increasing subscription costs, uncontrolled extensions, the need for manual workarounds, or the concentration of key knowledge in external partners.

Lifecycle Assurance Model for Cloud ERP

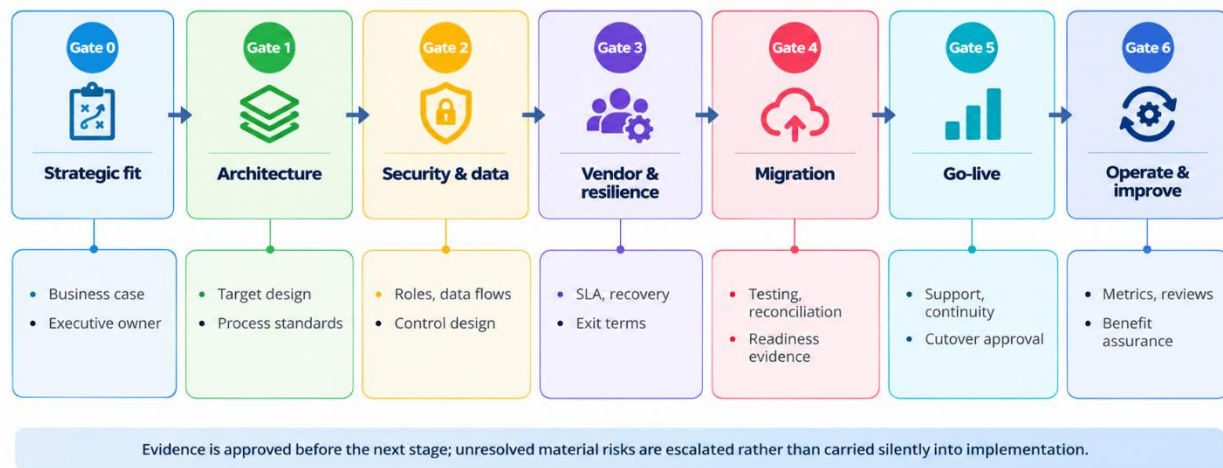


Figure 2. Seven-stage lifecycle assurance model linking cloud ERP decisions to evidence-based approval gates

Figure 2 turns these domains into a lifecycle assurance model which consists of seven stage-gates. Gate 0 checks that there is strategic fit and that there is executive ownership. Gate 1 approves the target architecture and the principles of process standardisation. Gate 2 verifies the design relating to data, identity, security and privacy. Gate 3 approves the vendor arrangements, the service-level agreements, the resilience plans and the exit arrangements. Gate 4 gives

authorization for migration following testing regarding configuration, integration, role, data and control. Gate 5 authorizes going live on the basis of operational readiness, support capacity, reconciliation and continuity arrangements. Gate 6 is responsible for ongoing improvement in the steady state by means of performance monitoring, access reviews, audit findings, release management, cost control, resilience exercises and benefit realization.

The stage-gate method deals with a typical weakness in governance, namely that controls are frequently examined too late, since once architectural and contractual decisions have been made they become expensive to alter. By linking evidence requirements to each decision point, assurance becomes a preventative measure. For instance, a security team should not find out during the final testing phase that the required segregation-of-duties model cannot be configured efficiently; procurement should not enter into a contract until the exit and incident obligations have been reviewed; and data owners should not come across problems relating to the quality of migration until the cutover takes place. The control matrix in Table 2 lists the example evidence and accountability for each area.

The framework also includes proportionality. It is not the case that all Saudi companies have the same size, level of regulatory exposure, or degree of process complexity. A smaller organisation can apply the same six domains using simpler evidence, whereas a large group will need formal architecture boards, risk committees, automated access governance, continuous controls monitoring, and several recovery tiers. Proportionality should aim at reducing bureaucracy rather than getting rid of accountability. The basic requirement is that every important decision, each critical data item, each privileged role, each external dependency, and each business continuity assumption must have a clearly identified owner and supporting evidence.

459

460

461 **Table 2. Governance control matrix for secure cloud ERP adoption.**

Governance domain	Minimum control expectation	Primary accountability	Representative evidence	KPI / trigger
Strategic decision rights	Approved business case, scope, risk appetite, exception authority	Executive sponsor / steering committee	Benefits baseline; decision log; risk acceptances	Benefit variance; overdue decisions
Architecture & integration	Approved target architecture and controlled interface/extension patterns	Enterprise architecture / application owner	Architecture map; interface register; release impact record	Failed interfaces; unmanaged customizations
Data governance	Named owners, classification, migration reconciliation, retention and lineage	Data owners / data governance lead	Data dictionary; migration sign-off; quality dashboard	Duplicate/error rates; unresolved reconciliation items
Identity, security & privacy	Strong authentication, least privilege, segregation of duties, logging and recertification	CISO/security + process owners	Role catalogue; access reviews; SoD analysis; security logs	Privileged exceptions; toxic combinations; stale accounts
Vendor &	Measurable SLA,	Vendor	SLA reports;	SLA

resilience	incident duties, recovery evidence, portability and exit capability	manager / continuity lead	recovery test; dependency map; exit plan	breaches; recovery gaps; concentration exposure
Capability & value assurance	Role training, support model, knowledge transfer, post-go-live review and cost control	Process owners / service owner	Training evidence; support KPIs; benefit review; cost report	Workarounds ; ticket trends; adoption gaps; cost drift

7. Discussion and Implications

The situation leads to three more general conclusions. Firstly, the adoption of a secure cloud ERP system is a matter of governance design. Although studies which examine adoption intention can help in spotting the perceived barriers, the fact that such intention exists does not prove that the controls, responsibilities, and recovery procedures are adequate. This is the reason why some studies find security to be statistically significant whereas others do not [14,15]. An organisation might be willing to go ahead with adoption even if its security governance is weak, or it might regard security as something manageable because it has confidence in the provider. Governance analysis must therefore shift from relying on perception to being based on evidence.

Secondly, cloud ERP systems modify rather than remove enterprise responsibility. Although the infrastructure operated by the provider can lessen the technical burden and enhance standardisation, the customer is still in charge of role design, process configuration, master-data quality, integration logic, approval structures, monitoring, and vendor oversight. The most serious failures are likely to take place at these organisational boundaries. This conclusion is in

line with research into digital transformation, which views technological and organisational change as inseparable [1-6], and with the Saudi ERP studies that stress the importance of leadership, culture, capability, and continuous support after go-live [19-23].

Thirdly, the alignment with Vision 2030 is most effective when cloud ERP develops into a measurable capability at the institutional level. Executives must be able to show how the platform enhances process visibility, service continuity, the quality of decisions, the reliability of control systems, and scalability. Cybersecurity and privacy should be presented as enabling conditions for trusted digital operations, not merely as compliance costs. The framework suggested enables the linking of transformation goals with control evidence and operational metrics, so that boards and executives can manage both value and risk throughout the same lifecycle.

For those involved, the framework states that assurance should be developed at the same time as the target operating model. In the business process workshops control owners and key data should be identified, architecture sessions should record the dependencies and failure modes, and procurement should convert the provider's claims into specific obligations. Internal audit and risk functions can then examine the evidence at the various gates rather than only doing so after implementation. This method also enhances accountability between the enterprise and the implementation partners since although consultants may set up the system, the process owners have to approve the resulting control logic and the business implications. Over time governance metrics can be included in the management dashboards so that items such as access exceptions, failed integrations, unresolved service breaches, data-quality defects and the results of recovery tests are displayed together with adoption and financial performance. It is important to carry out such integration since secure transformation needs continued management oversight after the project team has withdrawn without hindering business innovation.

8. Limitations and Future Research

507

508 The review is constrained by the fact that there are only a few studies which look at cloud ERP
509 governance in Saudi companies. In order to address this, the synthesis includes evidence from
510 Saudi ERP studies, evidence from Saudi cloud computing research, and international research on
511 cloud ERP. It is necessary to test the transferability rather than taking it for granted. Furthermore,
512 the corpus was limited to scholarly publications with DOIs published between 2020 and 2025, a
513 criterion which enhances the relevance and traceability of the information but might exclude
514 some relevant evidence from practitioners.

515

516 The framework should be assessed in future research by means of long-term case studies carried
517 out in Saudi companies covering the public sector, the industrial sector, the service sector, and
518 project-based organizations. Suitable measures for this purpose are control exceptions, the
519 reduction of access risk, recovery performance, integration incidents, improvements in data
520 quality, release stability, compliance with vendor services, user adoption, and the benefits that are
521 actually realized. Comparative studies should also examine whether governance requirements
522 differ in a material way according to the size of the enterprise, the cloud deployment model, the
523 ERP vendor, and the degree of process standardization.

524

525 **9. Conclusion**

526

527 Cloud ERP has the potential to help modernise Saudi enterprises by offering an integrated,
528 scalable, and constantly evolving digital core, but its value will only be realised if governance is
529 put in place to match the shift in control brought about by the cloud approach. The evidence
530 examined in this case demonstrates that security, architecture, data, vendors, resilience,
531 leadership, and organisational capability are interdependent. The six-domain, seven-gate
532 framework suggested here turns these interdependencies into accountable decisions and produces
533 auditable evidence. Its main idea is straightforward: secure adoption of cloud ERP is not

achieved by relying solely on technology, but rather by governing the entire process through which technology becomes an enterprise operating capability.

References

- [1] Verhoef, P.C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J.Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889-901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- [2] Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies*, 58(5), 1159-1197. <https://doi.org/10.1111/joms.12639>
- [3] Nadkarni, S., & Prugl, R. (2021). Digital transformation: A review, synthesis and opportunities for future research. *Management Review Quarterly*, 71, 233-341. <https://doi.org/10.1007/s11301-020-00185-7>
- [4] Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation*, 102, 102217. <https://doi.org/10.1016/j.technovation.2020.102217>
- [5] Kraus, S., Durst, S., Ferreira, J.J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management*, 63, 102466. <https://doi.org/10.1016/j.ijinfomgt.2021.102466>
- [6] Baiyere, A., Salmela, H., & Tapanainen, T. (2020). Digital transformation and the new logics of business process management. *European Journal of Information Systems*, 29(3), 238-259. <https://doi.org/10.1080/0960085X.2020.1718007>
- [7] Alsharari, N.M. (2020). Implementation of cloud ERP in the SME: Evidence from UAE. *Journal of Small Business and Enterprise Development*, 27(2), 299-327. <https://doi.org/10.1108/JSBED-01-2019-0007>

- [8] Alsharari, N.M. (2021). Institutional change of cloud ERP implementation in the public sector: A transformation of strategy. *International Journal of Disruptive Innovation in Government*, 1(1), 2-14. <https://doi.org/10.1108/IJDIG-03-2019-0002>
- [9] Alsharari, N.M. (2022). Cloud computing and ERP assimilation in the public sector: Institutional perspectives. *Transforming Government: People, Process and Policy*, 16(1), 97-109. <https://doi.org/10.1108/TG-04-2021-0069>
- [10] Salih, S., Hamdan, M., Abdelmaboud, A., Abdelaziz, A., Abdelsalam, S., Althobaiti, M.M., Cheikhrouhou, O., Hamam, H., & Alotaibi, F. (2021). Prioritising organisational factors impacting cloud ERP adoption and the critical issues related to security, usability, and vendors: A systematic literature review. *Sensors*, 21(24), 8391. <https://doi.org/10.3390/s21248391>
- [11] Awan, M., Ullah, N., Ali, S., Abbasi, I.A., Hassan, M.S., Khattak, H., & Huang, J. (2021). An empirical investigation of the challenges of cloud-based ERP adoption in Pakistani SMEs. *Scientific Programming*, 2021, 5547237. <https://doi.org/10.1155/2021/5547237>
- [12] Christiansen, V., Haddara, M., & Langseth, M. (2022). Factors affecting cloud ERP adoption decisions in organizations. *Procedia Computer Science*, 196, 255-262. <https://doi.org/10.1016/j.procs.2021.12.012>
- [13] Haddara, M., Gothesen, S., & Langseth, M. (2022). Challenges of cloud-ERP adoptions in SMEs. *Procedia Computer Science*, 196, 973-981. <https://doi.org/10.1016/j.procs.2021.12.099>
- [14] Haddar, H., & Bouaziz, F. (2022). Factors affecting cloud ERP adoption by Tunisian SMEs: A comparative study between adopters and non-adopters of traditional ERP. *International Journal of E-Adoption*, 14(1), 1-22. <https://doi.org/10.4018/IJEA.313913>
- [15] Qutaishat, F., Abushakra, A., Anaya, L., & Al-Omari, M. (2023). Investigating the factors affecting the intention to adopt cloud-based ERP systems during the COVID-19 era: Evidence from Jordan. *Business Process Management Journal*, 29(3), 653-670. <https://doi.org/10.1108/BPMJ-09-2022-0462>
- [16] Paulsson, V., & Johansson, B. (2023). Cloud ERP systems architectural challenges on cloud adoption in large international organizations: A sociomaterial perspective. *Procedia Computer Science*, 219, 797-806. <https://doi.org/10.1016/j.procs.2023.01.353>

- [17] Lee, C., Kim, H.F., & Lee, B.G. (2024). A systematic literature review on the strategic shift to cloud ERP: Leveraging microservice architecture and MSPs for resilience and agility. *Electronics*, 13(14), 2885. <https://doi.org/10.3390/electronics13142885>
- [18] Nguyen, N.D.K., Ali, I., Gupta, S., Chen, R., & Nareshe, B.S. (2024). Bridging the nexus between cloud ERP and enterprise resilience. *Journal of Global Information Management*, 32(1), 1-22. <https://doi.org/10.4018/JGIM.336556>
- [19] Bin Hammad, M.Z.M., Yahaya, J.B., & Mohamed, I.B. (2024). A model for enterprise resource planning implementation in the Saudi public sector organizations. *Heliyon*, 10, e24531. <https://doi.org/10.1016/j.heliyon.2024.e24531>
- [20] Mahmood, F., Khan, A.Z., Shah, S.A., & Adil, M. (2024). Post ERP implementation issues and challenges: Exploratory case studies in the context of Saudi Arabia. *Kybernetes*, 53(12), 5749-5774. <https://doi.org/10.1108/K-06-2022-0914>
- [21] Alkraihi, A.I., Jayawickrama, U., Olan, F., Asaduzzaman, M., Subasinghage, M., & Gallage, S. (2022). The perspective of national ERP vendors in achieving ERP project success in government organisations: A case of Saudi Arabia. *Enterprise Information Systems*, 16(1), 71-104. <https://doi.org/10.1080/17517575.2020.1845811>
- [22] Ali, M., Edghiem, F., & Alkhalifah, E.S. (2023). Cultural challenges of ERP implementation in Middle-Eastern oil & gas sector: An action research approach. *Systemic Practice and Action Research*, 36(1), 111-140. <https://doi.org/10.1007/s11213-022-09600-4>
- [23] Alsughayer, S. (2025). Role of ERP systems in management accounting in SMEs in Saudi Arabia. *Journal of Accounting & Organizational Change*, 21(2), 382-403. <https://doi.org/10.1108/JAOC-11-2022-0176>
- [24] Alghaith, W. (2023). The role of trust in cloud service providers on the adoption of cloud computing in Saudi Arabia: An empirical investigation. *Journal of Computer Science*, 19(9), 1107-1123. <https://doi.org/10.3844/jcssp.2023.1107.1123>
- [25] Ayadi, F. (2022). Critical factors affecting the decision to adopt cloud computing in Saudi health care organizations. *Electronic Journal of Information Systems in Developing Countries*, 88(6), e12231. <https://doi.org/10.1002/isd2.12231>

- 617 [26] Aldahwan, N.S., & Ramzan, M.S. (2021). Factors affecting the organizational adoption of
618 secure community cloud in KSA. *Security and Communication Networks*, 2021, 8134739.
619 <https://doi.org/10.1155/2021/8134739>
- 620 [27] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A
621 systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE*
622 *Access*, 9, 57792-57807. <https://doi.org/10.1109/ACCESS.2021.3073203>
- 623 [28] Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges
624 of cloud computing for government adoption: A systematic review. *International Journal of*
625 *Information Security*, 23, 1459-1475. <https://doi.org/10.1007/s10207-023-00797-6>
- 626 [29] Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A., & Kim, H. (2022). Security of zero
627 trust networks in cloud computing: A comparative review. *Sustainability*, 14(18), 11213.
628 <https://doi.org/10.3390/su141811213>
- 629 [30] Alquraish, M. (2025). Digital transformation, supply chain resilience, and sustainability: A
630 comprehensive review with implications for Saudi Arabian manufacturing. *Sustainability*,
631 17(10), 4495. <https://doi.org/10.3390/su17104495>