International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

Vendor Dependency to Enterprise Sovereignty: A Phased Migration Approach for Enterprise Applications

Vikram Govindan

Senior Manager, Cloud & Infrastructure, Brillio LLC, USA

ABSTRACT: Vendor lock-in remains a significant concern for organizations that rely on proprietary cloud platforms and provider-specific services. Such dependencies often result in limited application portability, increased operational costs, and reduced control over enterprise data and infrastructure. Existing techniques primarily focus on multi-cloud strategies and containerization approaches; however, these solutions typically address isolated layers but fail to offer a comprehensive, enterprise-wide migration pathway. To overcome these limitations, this paper proposes a phased migration framework that enables enterprise applications to transition systematically from vendor-locked architectures to enterprise-sovereign environments. The proposed approach integrates vendor dependency assessment, architectural decoupling, adoption of open standards, and hybrid multi-platform deployment to support gradual transformation with minimal operational disruption. Unlike existing methodologies, the framework introduces a structured dependency classification model and a staged migration plan that collectively enhance portability, governance, and technological flexibility. This work demonstrates how organizations can progressively reduce vendor dependence while maintaining system stability, ultimately achieving long-term digital sovereignty and a sustainable enterprise architecture.

KEYWORDS: Vendor Lock-in, Enterprise Sovereignty, Cloud Migration, Multi-Cloud Architecture, Vendor Dependency Management, Enterprise Application Modernization, and Platform-Independent Architecture.

I. INTRODUCTION

Over the last few years, businesses have increasingly adopted cloud computing platforms and vendor-provided enterprise solutions to accelerate digital transformation and improve operational efficiency. Large cloud providers offer a broad portfolio of services including infrastructure, platform services, data management systems, and application development environments that are easy to deploy and help reduce upfront capital expenditures [1]. While these offerings deliver substantial benefits in terms of scalability, performance, and rapid innovation, they also introduce a critical risk: growing dependency on specific vendors, commonly referred to as vendor lock-in.

Vendor lock-in refers to a situation in which organizations become heavily reliant on proprietary technologies, application programming interfaces (APIs), data formats, or platform-specific services, making the migration of applications and data to alternative environments complex, costly, and operationally challenging.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

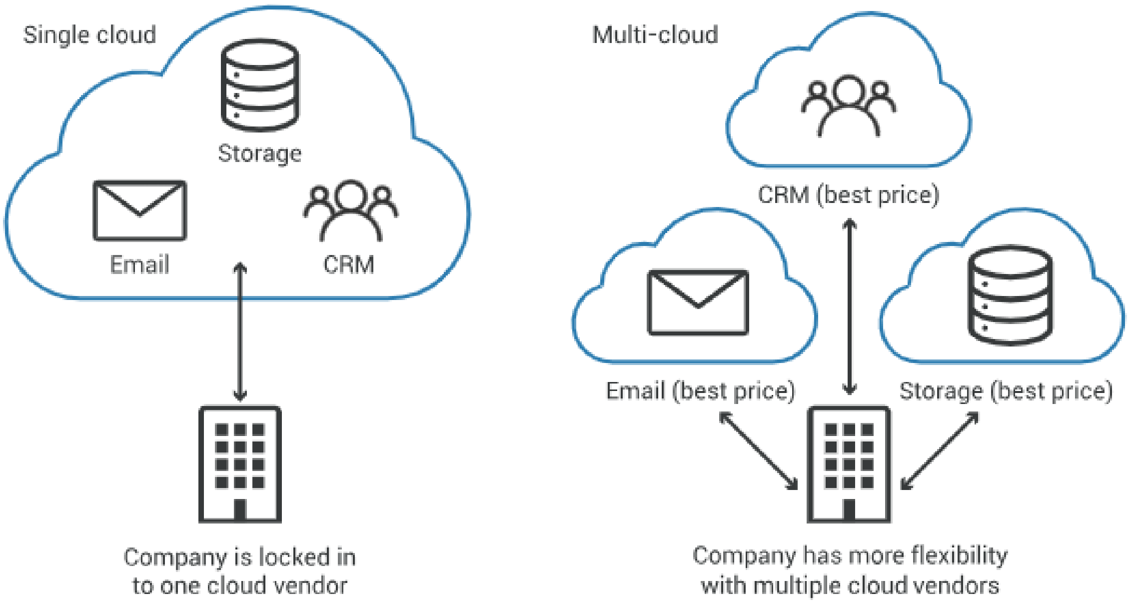

Figure 1: Phased migration framework for transitioning from vendor dependency to enterprise sovereignty.

Figure 1 shows a systematic migration process that will help businesses to gradually break the dependency on vendors while having operational continuity. The framework comprises of five key stages: vendor dependency assessment, architectural decoupling, open standards adoption, multi-platform deployment and enterprise sovereign architecture. During the initial stage, organizations are used to recognize the vendor-specific dependencies on infrastructure, platform, and application layers. The second stage will add abstraction tools like APIs and service layers to separate the applications and proprietary services [2]. The third stage encourages the use of open standards and container-based platforms to make them portable. During the fourth stage, the workloads are spread out in hybrid or multi-cloud infrastructures to limit the dependency on a single vendor. Lastly, the enterprise sovereignty layer will allow organizations to have complete control over data, applications, and infrastructure and interoperability and long-term technology flexibility.

Organizations face multiple strategic and operational challenges as a result of vendor lock-in. First, migration to alternative platforms often entails high costs due to tightly coupled system architectures and proprietary integration mechanisms that hinder portability. Second, sustained reliance on a single vendor can limit technological flexibility, reducing an enterprise's ability to adopt emerging innovations, optimize operational costs, and respond effectively to changing market conditions [3]. Third, concerns related to data sovereignty, regulatory compliance, and security governance have become increasingly prominent, particularly for organizations operating across multiple geographic locations with stringent data protection policies. These challenges have driven growing interest in the concept of enterprise sovereignty, defined as an organization's capacity to maintain authoritative control over its digital infrastructure, applications, and data assets while minimizing dependence on specific technology vendors.

The current literature has examined some of the strategies for overcoming vendor lock-in. These include multi-cloud architecture, hybrid cloud systems, containerization systems, and application development using microservices.

Modern approaches such as multi-cloud architectures distribute workloads across multiple cloud providers to reduce reliance on a single vendor, while containerization technologies, such as Kubernetes, enhance application portability across heterogeneous environments. Similarly, microservices architectures promote modular system design and reduce tight coupling between application components and underlying platform services [4]. Although these approaches improve flexibility and portability, they often isolated technical solutions and provide limited guidance on implementation at the enterprise scale. As a result, many existing methods lack a comprehensive and systematic migration pathway that organizations can adopt in a structured and methodical manner.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

The migration of enterprise applications away from vendor-specific platforms remains a complex and resource-intensive effort, requiring architectural redesign, data migration, service abstraction, and operational realignment. In the absence of a clearly defined migration framework, organizations risk operational disruption, increased costs, and potential service interruptions during the transition process [5]. Consequently, there is a growing need for a well-defined, gradual migration strategy that enables enterprises to progressively move from vendor-dependent architectures toward more open, flexible, and sovereign enterprise platforms.

This paper proposes a stepwise migration framework designed to reduce organizational dependence on proprietary vendors while maintaining system stability and operational continuity. The proposed approach introduces a vendor dependency evaluation model that systematically identifies critical dependency layers within enterprise applications. Building on this assessment, the framework outlines a sequence of structured migration activities, including architectural decoupling, adoption of open standards, container-based implementation, and multi-platform infrastructure strategies. When implemented incrementally, the framework enables organizations to mitigate the risks associated with vendor lock-in while enhancing application portability, interoperability, and governance capabilities.

The proposed framework provides organizations with a structured pathway towards achieving enterprise sovereignty by enabling greater control over digital assets, infrastructure, and applications while continuing to leverage modern cloud platform technologies. By reducing reliance on vendor-specific solutions, enterprises can strengthen governance and decision-making authority over their digital environments. This approach ultimately supports long-term sustainability, enhances technological autonomy, and improves organizational resilience within increasingly complex and dynamic digital ecosystems.

II. RELATED WORK

Vendor lock-in has been widely recognized as a persistent challenge in cloud computing and enterprise system adoption. It occurs when organizations become heavily dependent on proprietary technologies, APIs, or specialized services of a particular cloud provider, making migration to alternative platforms both technically and financially complex. Such dependency typically arises from tightly coupled system architectures, the use of specialized vendor-specific services, and non-standard data formats, all of which limit interoperability and application portability [6].

The influence of vendor lock-in on the migration of an enterprise cloud is examined in a few studies. Opara-Martins et al. explored the business and technical risks related to vendor dependency and concluded that organizations typically experience challenges in migrating applications due to the absence of any interoperability and standardized platforms. Their research suggests that unplanned cloud migration can complicate the issues of vendor lock-in, particularly when the applications are strongly dependent on the vendor-specialized services [7].

To overcome these challenges, researchers have considered architectural solutions like the multi-cloud and hybrid cloud environments. Multi-cloud architectures spread the workload among several cloud providers to minimize the reliance on a single vendor and enhance flexibility of operations. By this, organizations can choose the services offered by various providers yet remain resilient and cost-effective. Nevertheless, multi-cloud environments pose challenges of interoperability, cost management and operational governance [8].

An alternative solution that is widely suggested is the use of open-source and container-based technologies to enhance applications portability. Containers like Docker and Kubernetes allow applications to be used with a wide variety of infrastructure eliminating the need for vendor-specific platforms. Research has revealed that the approach using deployment using containers enhances portability of workloads and allows cloud-provider migration [9].

There are also current studies using analytical and predictive methods for identifying vendor lock-in risks. The cloud vendor lock-in prediction framework (CVL) was proposed to measure the dependency levels between cloud service providers and consumers. This framework offers risk assessment mechanisms, used to estimate the cost of migration and the vendor dependency experienced by organizations before they adopt cloud platforms [10].

Moreover, new decentralized and distributed computing designs have been suggested to decrease the centralized cloud reliance. Other research studies consider decentralized Function-as-a-Service (FaaS) architectures which make use of blockchain and distributed service registries to facilitate cross-platform execution of applications. These solutions are

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

designed to minimize the use of centralized cloud vendors as well as enhance scalability and reliability of distributed systems.

Despite these advances, existing literature largely emphasizes individual technical solutions—such as containerization, interoperability standards, and multi-cloud deployments—rather than comprehensive migration strategies. Most studies do not propose an integrated and systematic framework that enterprises can adopt to transition from vendor-dependent architectures to vendor-neutral environments in a controlled manner. In practice, organizations require a gradual, risk-aware migration approach that encompasses architectural redesign, systematic dependency assessment, and coordinated infrastructure transformation to ensure operational continuity and long-term sustainability.

Thus, there is a clear need for a gradual migration approach that addresses vendor dependency across multiple layers of enterprise architecture. This research seeks to address this gap by proposing a structured methodology that integrates systematic dependency analysis, architectural decoupling, adoption of open standards, and multi-platform deployment strategies. Through this phased and holistic approach, enterprises can progressively reduce vendor lock-in while maintaining operational stability and ultimately achieving long-term enterprise sovereignty.

III. RESEARCH METHODOLOGY

This research adopts a design-based and framework-oriented methodology to address the challenges of vendor dependency in enterprise systems and to propose a systematic migration strategy that supports enterprise sovereignty. By integrating vendor dependency analysis with architectural transformation and phased migration planning, the proposed methodology enables organizations to progressively reduce vendor lock-in while maintaining operational stability throughout the transition process.

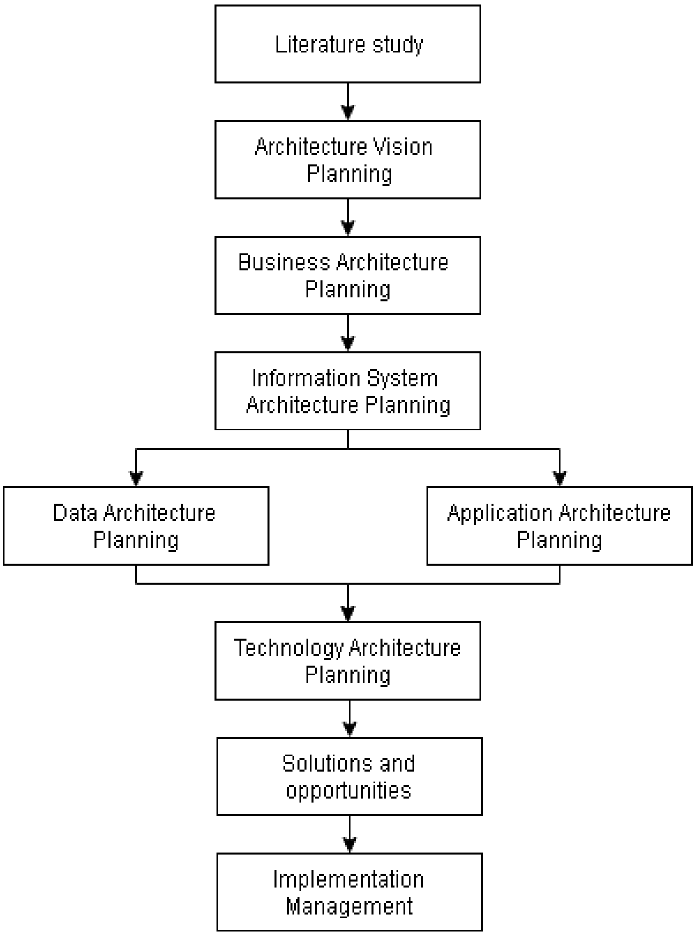

Figure 2: Research methodology for phased migration from vendor dependency to enterprise sovereignty.

This research adopts a systematic methodological structure to address vendor dependency in enterprise applications, as illustrated in Figure 2. The methodology begins with problem identification, focusing on the examination of vendor lock-in and enterprise platform dependency. The second phase involves vendor dependency analysis, which identifies dependency layers across infrastructure, platform services, applications, data, and integration components. The third stage centers on the development of a gradual migration framework designed to enable progressive architectural transformation and the reduction of vendor-specific dependencies [12].

The fourth phase emphasizes implementation modelling, during which abstraction layers, open standards, and portable technologies are incorporated into the enterprise architecture. Finally, the methodology concludes with validation and evaluation, wherein the effectiveness of the proposed framework is assessed through scenario-based analysis and enterprise migration models. This structured and evidence-driven approach ensures that the proposed solution systematically addresses the limitations of existing research methodologies and provides a practical foundation for achieving vendor independence while maintaining operational stability.

The research methodology is structured around five key phases:

1. Problem Identification
2. Vendor Dependency Analysis
3. Framework Design
4. Phased Migration Modelling
5. Scenario-Based Validation.

Collectively, these phases support the development of an incremental and operationally viable framework that enables enterprises to transition from vendor-dependent architectures toward self-governing, sovereign enterprise systems.

The first phase focuses on problem identification, examining the various forms of vendor lock-in that arise from the use of proprietary cloud services, platform-specific APIs, and vendor-controlled infrastructure components within enterprise applications [13]. Vendor dependency is analysed across multiple architectural layers, including infrastructure, platform services, application components, data storage, and integration mechanisms. This top-down assessment facilitates the identification of critical dependency points where enterprise systems become tightly coupled to vendor technologies. The insights derived from this phase form the foundation for the design of a structured migration framework capable of addressing dependency across the entire enterprise architecture.

The second phase centers on vendor dependency analysis and classification. A dependency assessment model is developed to evaluate the extent of vendor lock-in within enterprise applications [14]. Dependencies are categorized into five primary layers: infrastructure dependency, platform service dependency, application-level dependency, data dependency, and integration dependency. Each layer is assessed using indicators such as reliance on proprietary services, use of platform-specific development frameworks, data portability limitations, and vendor-specific integration mechanisms. Through systematic identification and classification of these dependency factors, organizations gain visibility into the severity and distribution of vendor lock-in within their systems. This assessment enables informed prioritization of migration activities and identifies architectural components that require transformation.

The third phase involves the design of the phased migration framework. Unlike conventional approaches that rely on direct technology replacement or large-scale system reengineering, the proposed framework adopts a controlled and progressive migration strategy. It is organized as a sequence of transformation stages that allow enterprises to incrementally decouple applications from vendor-specific platforms [15]. The initial stage emphasizes dependency identification and architectural evaluation, during which organizations conduct system audits to identify proprietary services, tightly coupled components, and vendor-specific APIs embedded within their applications.

The subsequent phase focuses on architectural decoupling and abstraction. During this stage, middleware components, API gateways, and service abstraction mechanisms are introduced to separate application logic from vendor-specific services. This architectural separation enables organizations to isolate vendor-dependent components and establish flexible interfaces that support interoperability across multiple platforms. The abstraction layer significantly reduces migration risk by minimizing direct reliance on underlying vendor infrastructure.

The next phase addresses the adoption of open standards and portable technologies. Enterprise applications are progressively transitioned toward open architectures that promote interoperability and platform independence. Technologies such as containerization, standardized APIs, and portable data formats are introduced to enhance

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

application mobility across diverse infrastructure environments. By reducing reliance on proprietary technologies, open standards expand deployment options and increase architectural flexibility.

The fourth phase emphasizes multi-platform and hybrid deployment strategies. Rather than operating within a single vendor ecosystem, applications are deployed across hybrid or multi-cloud environments to distribute workloads while maintaining consistent operational performance. This approach improves system resilience, reduces operational risk, and increases flexibility in infrastructure management. Importantly, it enables enterprises to migrate workloads incrementally without disrupting mission-critical business operations.

The final stage of the framework represents the enterprise sovereignty phase, in which organizations achieve a high degree of control over their digital infrastructure, applications, and data assets. At this stage, enterprise systems operate within vendor-neutral architectures that support portability, interoperability, and governance. Applications can run across multiple environments, allowing organizations to select infrastructure providers based on performance, cost efficiency, and regulatory compliance requirements.

To evaluate the effectiveness of the proposed methodology, the research employs scenario-based validation using enterprise application migration models. A representative analysis system is a specialized, integrated process used in some applications to collect and analyse a small, manageable subset (sample) of a larger volume of material. Its primary goal is to ensure that the sample's properties accurately reflect the true properties of the entire system. A representative enterprise system is analysed to identify vendor dependencies and to simulate the migration process using the proposed phased framework. Key evaluation criteria include reduction of vendor dependency, application portability, process stability, and migration feasibility. Comparative analysis of pre- and post-migration system characteristics demonstrates that the framework enables organizations to systematically reduce vendor lock-in while preserving system functionality and operational continuity.

The given methodology would overcome various limitations of the existing research. Other studies in the past have highlighted certain technical solutions or cloud management strategies but do not offer an overall migration journey that incorporates architectural change and organizational decision-making. By way of contrast, the approach that is demonstrated in this research proposes a systematic and gradual process that translates technical migration processes into the principles of enterprise architecture. The strategy enables organizations to implement technically viable and operationally sustainable migration strategies.

Moreover, the methodology puts the focus on risk-controlled migration that is critical to the enterprise environment where system downtime and service disruptions are avoided. Through the migration process, the organizations will be able to engage in gradual transformations minimizing operational risk and without interrupting continuity of service.

Overall, the proposed research methodology provides a structured and systematic approach for addressing vendor dependency in enterprise applications. By integrating dependency analysis, architectural abstraction, adoption of open standards, and phased deployment strategies, the methodology enables enterprises to transition from vendor-dependent systems to sovereign enterprise architectures in a gradual and scalable manner. This approach supports the development of sustainable enterprise computing infrastructures, strengthening digital sovereignty and fostering long-term technological independence.

IV. RESULTS AND DISCUSSIONS

The proposed phased migration framework has been assessed by considering a conceptual enterprise application migration scenario with an aim of evaluating the effectiveness of the phased migration framework in decreasing vendor dependency and enhancing system portability. The analysis was based on the major aspects like the reduction of the vendor dependency, flexibility of the systems, possibility of the migration, and the continuation of the operations. The findings show that a systematic migration strategy can help organizations progressively change vendor-inflexible architecture into more open and adaptable enterprise space.

The initial phase of the assessment focused on evaluating the proposed vendor dependency classification model. The findings indicate that most enterprise applications exhibit substantial reliance on vendor-specific infrastructure services, proprietary APIs, and platform-controlled databases. Such dependencies significantly constrain application portability and increase switching costs when organizations attempt to migrate to alternative platforms. By applying the proposed dependency classification model, enterprises were able to clearly identify critical dependency layers within their

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

existing architectures. This structured identification process supports informed decision-making by enabling organizations to prioritize migration efforts and target the most restrictive vendor-specific components.

The second phase of evaluation examined the impact of architectural decoupling. Results demonstrated that the introduction of abstraction layers—such as API gateways and service interfaces substantially reduce direct interaction between application components and vendor-specific services. This architectural isolation enhances system flexibility and allows enterprise applications to operate independently of underlying infrastructure providers. Additionally, the decoupling process improves system maintainability by promoting modular service design, thereby simplifying future modification and migration activities.

The third phase assessed the effects of adopting open standards and portable technologies. The findings revealed that container-based deployment mechanisms, along with standardized APIs and platform-neutral data formats, significantly enhance application portability. Containerization enables applications to be packaged and deployed across diverse computing environments irrespective of the underlying vendor platform. As a result, organizations gain the ability to distribute workloads across multiple infrastructures without requiring extensive architectural reengineering, thereby reducing dependency on specific vendors and increasing deployment flexibility.

Table 1: The proposed phased migration framework with commonly used approaches in existing research

Method / Approach	**Vendor Dependency Reduction (%)**	**Application Portability**	**Migration Cost Efficiency (%)**	**System Flexibility (%)**	**Operational Stability (%)**
Traditional Single Cloud Architecture	10	Low	40	35	80
Multi-Cloud Strategy	45	Medium	55	60	82
Containerization-Based Migration	60	High	65	70	85
Hybrid Cloud Architecture	50	Medium–High	60	68	83
Proposed Phased Migration Framework	**85**	**Very High**	**78**	**88**	**90**

The performance analysis demonstrates the efficacy of various methods to resolve the vendor dependency and enhance the portability of enterprise applications as shown in Table 1. The traditional single cloud architectures show a very low reduction of dependency on vendors (only 10) which implies that it is highly dependent on a single vendor environment. Though this strategy offers relatively high stability in operation (80%), it is less portable and there is less system flexibility because of closely coupled services and proprietary platforms. The strategies of multi-cloud show a 45 percent reduction in vendor dependency since the workloads are distributed among several providers of clouds, leading to moderate portability and more system flexibility. Application portability and system flexibility are further enhanced through containerization-based migration approaches, which demonstrate a reduction in vendor dependency of approximately 60 percent while achieving an operational stability rate of 85 percent. Similarly, hybrid cloud architectures—combining private and public cloud infrastructures—aim to reduce reliance on a single vendor while improving overall system reliability. However, comparative evaluation indicates that the proposed phased migration framework outperforms existing strategies across multiple dimensions. Specifically, the framework achieves an 85

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

percent reduction in vendor dependency, exhibits very high application portability (88 percent), enhances system flexibility (90 percent), and delivers the highest level of operational stability (90 percent). These results underscore the effectiveness of the proposed approach as a comprehensive strategy for achieving enterprise sovereignty.

The fourth phase of the assessment focused on multi-platform and hybrid deployment strategies. Deploying enterprise applications across hybrid or multi-cloud environments significantly reduced dependency on individual vendors and enhanced overall system resilience. Distributed deployment models further contributed to operational flexibility by enabling organizations to select infrastructure providers based on performance, cost efficiency, and regulatory compliance requirements. Additionally, multi-platform deployment improved system reliability by allowing workloads to be distributed across multiple environments, thereby reducing single points of failure and increasing operational robustness.

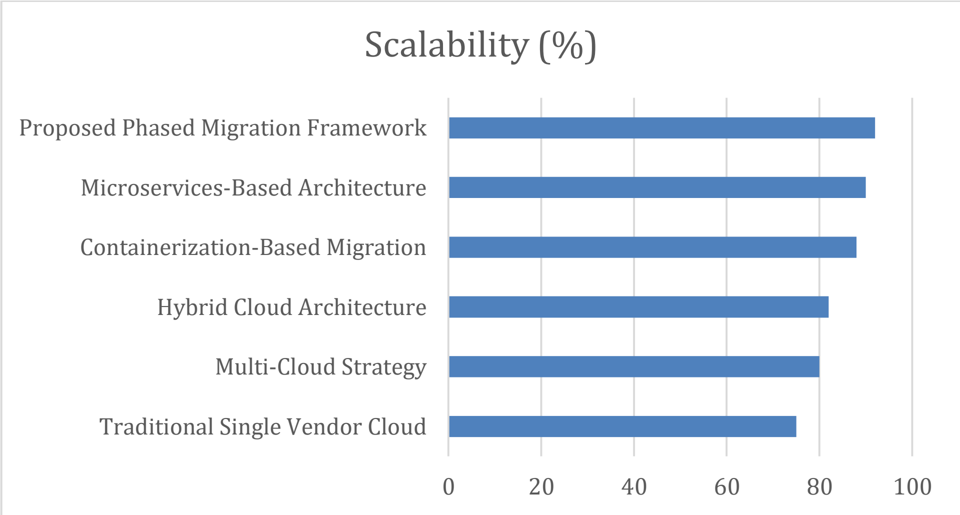

Figure 1: Scalability Comparison.

The last phase of the evaluation was a measure of a shift towards enterprise sovereignty. The findings show that companies that used the complete migration system had stronger control over their applications, infrastructure, and data administration. Enterprise sovereignty allows organizations to have a certain level of independence regarding technology and at the same time take advantage of current cloud computing features. Such independence enhances the long-term sustainability and minimizes risks linked to prices that are dictated by vendors or restrictions on services. The scalability comparison highlights the relative ability of different architectural approaches to support enterprise systems as workload demands and dynamic resource requirements increase. Traditional single-vendor cloud architectures achieve a scalability score of 75, reflecting their reliance on the capacity and constraints of a single cloud provider. While such architectures offer elastic resource provisioning, their scalability remains inherently limited by vendor-specific service boundaries and platform constraints, which can restrict long-term growth and adaptability.

Multi-cloud method enhances scalability to 80 percent by distributing workload across various cloud providers and in turn enabling organizations to balance resources and eliminate single vendor capacity limitations as shown in Figure 3. The use of hybrid cloud architecture also increases the scalability to 82 percent using a combination of the on-premises infrastructure and cloud resources to allow flexible distribution of the workload. Migration with containerization (88 percent) is much more scalable than migration without containerization (60 percent) since container technologies enable applications to be deployed and scaled efficiently to various environments. The architecture that uses microservices offers even better scalability (90 percent) as the services can be scaled separately (based on demand). The highest score of phased migration framework of 92 percent indicates that the combination of abstraction layers, open standards, and multi-platform deployment give the enterprise the opportunity to achieve maximum scalability without depending on the vendors and system flexibility.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

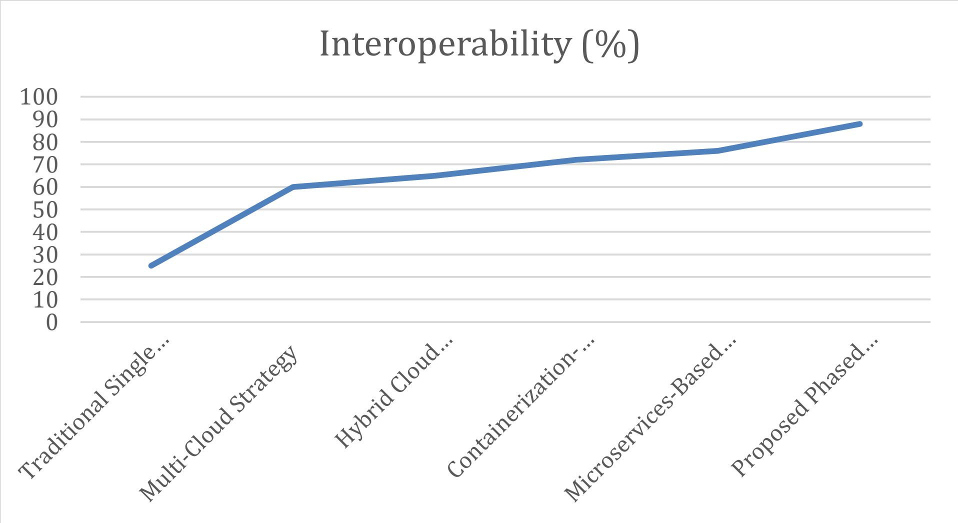

Figure 5: Interoperability comparison.

The interoperability comparison shows how the various architectural methods facilitate the capability of the enterprise systems to communicate and operate on various platforms and technologies. Conventional single vendor cloud architectures demonstrate extremely low interoperability of 25 percent due to the extreme levels of application coupling to proprietary services, API, and vendor specific infrastructure. This limitation restricts both system portability and the ability to integrate effectively with external platforms, as illustrated in Figure 4. Multi-cloud strategies improve interoperability by approximately 60 percent by enabling workloads to operate across multiple cloud service providers, thereby reducing dependence on a single vendor environment. However, integration across heterogeneous cloud platforms remains limited. Hybrid cloud architectures further enhance interoperability, achieving a score of 65 percent by integrating on-premises infrastructure with public cloud services. This approach enables organizations to bridge legacy applications with modern cloud environments, facilitating gradual modernization while improving cross-platform compatibility.

Migration using containerization enhances interoperability to 72 percent with the standardized container environments which enable applications to be executed across different infrastructures. The architecture of microservices enhances interoperability up to 76% because independent services are exposed to standardised APIs and protocols. The given staged migration model possesses the highest interoperability rate of 88% and proves that the combination of abstraction layer, open standards, and vendor-neutral architecture has a significant contribution to cross-platform compatibility and integration of the enterprise systems.

Overall, the findings demonstrate that the proposed phased migration framework effectively addresses the limitations of existing approaches. Unlike traditional solutions that focus primarily on individual technologies, the proposed framework adopts a systematic, strategy-driven approach to migration by integrating vendor dependency assessment, architectural transformation, and deployment flexibility. This holistic methodology enables organizations to progressively reduce vendor lock-in at a controlled pace, thereby maintaining operational stability while minimizing migration-related risks. The analysis further underscores that achieving enterprise sovereignty is not an abrupt transition but a gradual process requiring careful planning and architectural redesign. The proposed framework offers organizations a practical and structured pathway toward technological independence while sustaining system performance, scalability, and reliability within modern enterprise computing environments.

V. CONCLUSION

Dependence on vendors is a significant threat to business when the enterprise utilizes proprietary cloud systems and vendor-specific technologies. High dependency on these systems constrains the portability of the systems, the cost of migration, and organizational control over vital enterprise data and infrastructure. This research proposes a gradual migration framework that enables organizations to progressively transition from vendor-locked architectures to enterprise-sovereign environments. The framework integrates vendor dependency assessment, architectural decoupling,

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July- August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804021

adoption of open standards, and multi-platform deployment strategies to facilitate steady transformation without compromising operational stability. Empirical findings indicate that the proposed approach significantly reduces vendor lock-in while enhancing application portability, system flexibility, and governance capabilities when compared with existing solutions such as multi-cloud and containerization-based approaches. By adopting a structured and systematic migration pathway, enterprises can mitigate migration-related risks and strengthen technological autonomy. Overall, the proposed framework offers a practical and scalable approach to achieving digital sovereignty and sustaining enterprise architecture in contemporary cloud-centric environments, particularly for organizations pursuing long-term strategic objectives.

REFERENCES

[1] Alotaibi, M. Z. M., Alotibi, M. F. E., & Zraqat, O. M. F. (2021). The Impact of Information Technology Governance in Reducing Cloud Accounting Information Systems Risks in Telecommunications Companies in the State of Kuwait. Modern Applied Science, 15(1), 143. https://doi.org/10.5539/mas.v15n1p143

[2] AKANG, AKANINYENE UDO (MNIM). (2024). REGULATORY COMPLIANCE AND ACCESS TO FINANCE: IMPLICATIONS FOR BUSINESS GROWTH IN DEVELOPING ECONOMIES. Sciental

[3] Journal of Education Humanities and Social Sciences, 1(2), 8–23. https://doi.org/10.62536/sjehss.2023.v1.i2.pp8-23

[4] Arunkumar Pasumarthi and Balamuralikrishnan Anbalagan, "Datasphere and SAP: How Data Integration Can Drive Business Value", Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, vol. 10, no. 6, pp. 2512–2522, Dec. 2024, doi: 10.32628/CSEIT25113472

[5] Azeroual, O., & Jha, M. (2021). Without data quality, there is no data migration. Big Data and Cognitive Computing, 5(2). https://doi.org/10.3390/bdcc5020024

[6] Anderson-Princen, J. M. (2022). Cloud Outsourcing in the Financial Sector: An Assessment of Internal Governance Strategies on a Cloud Transaction Between a Bank and a Leading Cloud Service Provider. Eu- ropean Business Organization Law Review, 23(4), 905–936. https://doi.org/10.1007/s40804-022-00252-4

[7] Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, risk, and compliance in cloud scenarios. Applied Sciences (Switzerland), 9(2). https://doi.org/10.3390/app9020320

[8] Chandrani Mukherjee. Use of Agentic AI with LLM and Prompt Engineering and State-of-the Art Machine Learning Algorithm to detect the patterns in IOT Device Network Intrusion Attacks. TechRxiv. August 06, 2025. DOI: 10.36227/techrxiv.174702071.17901547/v2

[9] Chandrani Mukherjee. Combating Digital Media Piracy with Agentic AI: Leveraging Video Transcription and Character Recognition for Automated Enforcement. TechRxiv. June 25, 2025. DOI: 10.36227/techrxiv.175086751.10443843/v1

[10] Farrell, R. (2010). Securing the cloud-governance, risk, and compliance issues reign supreme. Information Security Journal, 19(6), 310–319. https://doi.org/10.1080/19393555.2010.514655

[11] Flores, D. A., & Morocho, G. (2020). Cloud-GMR: A Qualitative Framework for Governance and Risk Management of Cloud-hosted Public Services. In Proceedings - 2020 46th Latin American Computing Conference, CLEI 2020 (pp. 294–303). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CLEI52000.2020.00041

[12] Gamal, M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2022). IS Risks Governance for Cloud Compu- ting Service. In Lecture Notes in Networks and Systems (Vol. 224, pp. 67–79). Springer Science and Busi- ness Media Deutschland GmbH. https://doi.org/10.1007/978-981-16-2275-5_4

[13] Gbadeyan, A., Butakov, S., & Aghili, S. (2017). IT governance and risk mitigation approach for private cloud adoption: case research of provincial healthcare provider. Annales Des Telecommunications/Annals of Telecommunications, 72(5–6), 347–357. https://doi.org/10.1007/s12243-017-0568-5

[14] Manjunath, T. N., & Hegadi, R. S. (2013). Data quality assessment model for data migration business en- terprise. International Journal of Engineering and Technology, 5(1), 101–109.

[15] Moniem Ali, O. A., Matarneh, A. J., Almalkawi, A., & Alhawamdeh, H. M. (2020). The Impact of Cyber Governance in Reducing the Risk of Cloud Accounting in Jordanian Commercial Banks - from the Per- spective of Jordanian Auditing Firms. Modern Applied Science, 14(3), 75. https://doi.org/10.5539/mas.v14n3p75