Int. j. adv. multidisc. res. stud. 2025; 5(6):2471-2485

Received: 10-11-2025
Accepted: 20-12-2025

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

IT Services Decoupling After Mergers, Acquisitions, and Ownership Transitions: A Framework for Secure Infrastructure Separation

[1] Samuel Fadero, [2] Demilade Jooda, [3] Serif Oyindamola Oyesiji, [4] Stanley Nwakamma

[1] SanlamAllianz Life Insurance Ltd, Lagos, Nigeria
[2] Goldman Sachs - Dallas, Texas, United States
[3] Independent Researcher, Lagos, Nigeria
[4] Independent Researcher, United States of America

DOI: https://doi.org/10.62225/2583049X.2025.5.6.6803
Corresponding Author: **Samuel Fadero**

Abstract

This review examines the secure separation of information technology services following mergers, acquisitions, divestitures, and ownership transitions, with particular attention to complex, geographically distributed corporate environments. Its purpose is to establish a structured framework for achieving operational independence while preserving cybersecurity, service continuity, data integrity, regulatory compliance, and commercial control. The study adopts a structured narrative review, synthesising peer-reviewed literature, recognised frameworks, and applied lessons from a USD 1.5 million decoupling programme. The analysis addresses pre-separation discovery, dependency mapping, infrastructure baselining, governance, identity and access reconfiguration, network and cloud separation, application and data disentanglement, Transitional Service Agreements, vendor and licensing dependencies, migration execution, testing, cutover management, and performance evaluation. Findings indicate that successful decoupling depends less on physical asset movement than on disciplined management of interdependencies, trust boundaries, ownership rights, operational readiness, and residual commercial obligations. The review further demonstrates that measurable service autonomy requires rigorous governance, accountable stakeholders, controlled migration sequencing, post-cutover assurance, and evidence-based performance metrics encompassing cost, schedule, security, resilience, and business continuity. Emerging capabilities, including digital twins, artificial intelligence, automated orchestration, and real-time observability, may strengthen future separation programmes when governed appropriately. The study concludes that secure decoupling should be treated as an enterprise lifecycle capability rather than a one-off technical exercise. It recommends maintaining authoritative asset inventories, formalising separation playbooks, strengthening identity governance, defining time-bound TSA exit criteria, institutionalising lessons learned, and advancing empirical research on maturity, automation, residual dependency risk, and long-term operating independence. These recommendations are pertinent in emerging markets, where infrastructure constraints, regulatory variation, skills shortages, and vendor concentration intensify transition risk.

Keywords: IT Decoupling, Infrastructure Separation, Mergers and Acquisitions, Transitional Service Agreements, Cybersecurity Governance, Operational Resilience

1. Introduction

1.1 Mergers, Acquisitions, and the Imperative for IT Separation

Mergers, acquisitions, divestitures, and ownership transitions are justified by expected gains in scale, market access, capability acquisition, and portfolio restructuring; however, realization of those gains depends on information technology. Contemporary enterprises embed business processes in applications, identity services, networks, data platforms, cloud environments and outsourced technology arrangements, making IT inseparable from transaction execution. Evidence that cross-business IT integration capability contributes to acquirer value indicates that technology decisions are not merely post-deal administrative matters but determinants of whether anticipated synergies become operating performance (Tanriverdi & Uysal, 2011) [68].

The imperative becomes acute where a transaction requires organizational separation rather than full absorption. A carve-out

may oblige the seller to disentangle infrastructure integrated over many years to provide shared services. Research on multinational carve-outs demonstrates that systems must often be separated under compressed timelines while satisfying operational and compliance requirements, placing IT on the transaction's critical path (Fähling *et al*., 2013) [21]. Separation must therefore be treated as an engineered transformation rather than a simple transfer of hardware or user accounts.

The central difficulty is that the desired post-transaction operating model may differ fundamentally from the pre-transaction architecture. Research on post-merger IT strategies shows that the degree of technology integration should follow the strategic ambition of the deal rather than a universal preference for maximum consolidation (Wijnhoven *et al*., 2006) [74]. The same logic applies inversely to divestitures: the target state must define which services remain shared temporarily, which capabilities migrate, which assets are duplicated and which dependencies must be eliminated to achieve operational autonomy.

Poorly configured technology transitions can destroy rather than create value. A configurational analysis of problematic M&A integrations demonstrates that deficiencies emerge from interacting technical, organizational and contextual conditions, including inappropriate integration choices and failure to preserve essential business capabilities (Henningsson & Kettinger, 2016) [32]. This supports early separation design in which infrastructure, applications, data, security controls and operating responsibilities are mapped before contractual and cutover commitments become difficult to reverse.

Successful post-M&A information-system integration also depends on identifying critical functions, preserving pre-transaction knowledge and avoiding standardization disconnected from business requirements (Chang, Chang & Wang, 2014) [18]. For infrastructure separation, these principles translate into dependency discovery, service criticality assessment, architecture baselining and explicit ownership decisions. The objective is not simply to disconnect environments, but to preserve required capabilities while ensuring that the new entities no longer depend on inappropriate shared systems.

This is important in regulated and technology-intensive sectors. Banking research shows that effective M&A IT execution requires governance, integration planning, architecture decisions and attention to operational and technology risks throughout the transaction lifecycle (Kovela & Skok, 2015) [40]. Such requirements also apply to ownership transitions in which access rights, customer information, privileged credentials, or regulatory records must move between independently governed entities without producing service outages or residual unauthorized access.

Cybersecurity makes separation more urgent. Empirical evidence indicates that M&A activity can be associated with increased cybersecurity risk, particularly where transactions involve intangible and technology-dependent assets (Vu, Hoang & Hoang, 2024) [72]. Transitional environments may create duplicated identities, temporary network pathways, unclear asset ownership, and inconsistent security controls. Secure decoupling must therefore establish new trust boundaries, revoke inherited privileges, segregate monitoring responsibilities and prevent temporary connectivity from becoming a persistent attack path.

The strategic relevance is also visible in African financial markets. Evidence from Sub-Saharan African banking shows that mergers do not automatically improve post-transaction profitability, reinforcing the proposition that transaction value depends on execution quality rather than deal completion alone (Ayagre *et al*., 2024) [15]. In Nigeria, banking-sector M&A research likewise demonstrates organizational and human-resource consequences, highlighting the need for coordinated change management alongside technical restructuring (Gomes *et al*., 2012) [29].

The strongest case for IT separation comes from divestor-centric research showing that carve-out complexity increases the time required to achieve physical separation and can leave stranded IT assets that weaken post-divestment alignment and performance (Yetton *et al*., 2023) [76]. Secure decoupling should therefore begin during transaction planning and proceed through dependency discovery, target-state architecture, data and identity separation, controlled migration, validation and decommissioning. This logic aligns with a USD 1.5 million decoupling programme: investment should be judged not only by systems moved, but by whether service independence, security, continuity and ownership clarity are demonstrably achieved.

1.2 Complexity and Risk in Transitional IT Environments

Transitional IT environments created by mergers, acquisitions, divestitures and ownership changes are intrinsically complex because technology must continue supporting business operations while architectures, responsibilities and control boundaries are being redefined. During this period, organisations frequently operate overlapping applications, duplicate identities, temporary interfaces and parallel infrastructure, increasing the number of dependencies that must be understood and governed. Research on M&A information-system integration identifies legacy-system management, security, competence, communication and executive support as critical because weaknesses in any of these areas can destabilise the transition (Johansson, Waldau & Åhlström, 2023) [36].

Complexity is intensified by the interaction between strategic objectives and technical constraints. IT systems embody processes, data structures and organisational routines; consequently, hurried consolidation or separation can interrupt workflows, degrade service quality and generate unplanned costs. The performance literature therefore treats technology compatibility, integration planning and sequencing as material determinants of post-transaction outcomes rather than secondary implementation concerns (Lohrke, Frownfelter-Lohrke & Ketchen, 2016) [42]. Moreover, M&A integration evolves dynamically as transaction priorities, organisational structures and technical knowledge change, requiring management mechanisms capable of adjusting decisions throughout the transition lifecycle (Henningsson & Carlsson, 2011) [31].

Operational continuity is especially important in sectors where customers depend on uninterrupted digital services. Nigerian banking evidence shows that post-merger performance is shaped by technological integration, communication and cultural alignment, illustrating how service disruption can emerge when organisational and technical transitions are insufficiently coordinated (Mammah & Hassan, 2022) [44]. In other African contexts,

the relationship between IT investment and performance is not automatically linear. Evidence from Ghanaian banks indicates that technology expenditure does not invariably translate into improved efficiency, underscoring the importance of governance, utilisation and implementation quality during transitional programmes (Boadi *et al*., 2022) [17].

Risk also extends beyond internally controlled infrastructure. Transitional arrangements commonly depend on cloud providers, shared platforms and outsourced services that may remain temporarily connected to the former or acquiring entity. Financial-sector cloud research demonstrates that weak internal controls, regulatory uncertainty and transaction misalignment can create residual legal, technological and governance exposure in third-party arrangements (Anderson-Princen, 2022) [13]. Accordingly, secure infrastructure separation requires transition teams to treat temporary states as deliberate architectures: dependencies should be documented, access rights time-bounded, shared services governed, data flows monitored and exit criteria defined. For a major decoupling programme, these practices reduce the probability that transitional convenience becomes permanent technical debt or that unresolved dependencies compromise security, autonomy and service continuity across complex, geographically dispersed corporate operating environments at organisational scale.

1.3 Aim, Scope, and Review Approach

This review aims to develop a rigorous understanding of how IT services can be securely decoupled following mergers, acquisitions, divestitures, and ownership transitions, with particular emphasis on preserving operational continuity while establishing independent technology environments. The study focuses on the strategic, architectural, operational, cybersecurity, and governance dimensions of separation, recognising that successful decoupling extends beyond physical infrastructure migration to include applications, identities, data, networks, cloud services, vendor relationships, licensing arrangements, and transitional dependencies.

The scope encompasses pre-separation discovery, dependency mapping, infrastructure baselining, governance structures, identity and access reconfiguration, network and cloud separation, application and data disentanglement, Transitional Service Agreements, cutover management, testing, stabilisation, and post-separation performance evaluation. Particular attention is given to the practical complexities that arise where legacy platforms, shared services, regulatory obligations, and geographically distributed operations must be separated under time, cost, and risk constraints. The review also draws applied insight from a USD 1.5 million decoupling programme to connect scholarly evidence with implementation realities without disclosing confidential organisational information.

Methodologically, the paper adopts a structured narrative review approach, synthesising peer-reviewed literature, recognised frameworks, and relevant practitioner evidence. Sources are examined comparatively to identify recurring risks, control mechanisms, sequencing principles, and critical success factors. This approach enables the study to integrate conceptual understanding with applied programme lessons and to formulate a secure, phased framework for infrastructure separation that is adaptable across transaction types, organisational scales, and technology environments. It further provides a basis for evaluating service independence, residual dependencies, governance effectiveness, and resilience.

2. IT Services Decoupling in Post-Transaction Corporate Environments

IT services decoupling is the structured process through which technology capabilities that previously operated within a shared corporate environment are separated into independently governable service domains following a divestiture, acquisition, carve-out, or ownership transition. Unlike conventional post-merger integration, which normally seeks increasing technological commonality, decoupling seeks controlled autonomy. The target state therefore requires explicit decisions concerning which applications, networks, identities, data repositories, infrastructure services and contracts should migrate, be replicated, remain temporarily shared or be retired. M&A technology guidance consequently treats architecture choice as inseparable from transaction strategy because preservation, consolidation, combination and transformation models generate materially different requirements for technology execution (Blatman & Lukac, 2013) [16].

A principal challenge is that corporate IT environments accumulate interdependencies long before separation becomes commercially necessary. Shared databases may support several business units; enterprise applications may depend on common directories; networks may carry traffic for multiple legal entities; and vendor agreements may cover infrastructure that cannot be cleanly attributed to one owner. The M&A information-systems literature shows that integration outcomes depend on numerous interacting decisions concerning architecture, governance, organisational context and implementation method, illustrating why reversal of established integration can be exceptionally demanding (Henningsson, Yetton & Wynne, 2018) [34].

Decoupling should therefore be understood as capability reconstruction rather than simple disconnection. IT resources are not necessarily scale-free or readily transferable between organisations; asymmetries in technology capabilities can make integration costly and reduce anticipated transaction value when resources cannot be transferred without substantial adaptation (Tanriverdi & Uysal, 2015) [69]. The inverse is equally relevant to separation: an apparently transferable application may remain dependent on shared authentication, middleware, interfaces, licences or specialist personnel. A credible separation design must therefore define service boundaries at the level of dependencies rather than merely at the level of asset ownership.

Human knowledge also becomes a separation dependency. Acquisition research demonstrates that external specialists can provide scarce integration expertise, yet organisations must balance temporary external capability against retention of internal knowledge required after transition (Henningsson & Øhrgaard, 2015) [33]. For a decoupling programme, this implies that infrastructure engineers, application owners, cybersecurity personnel, vendors and business-process specialists should collectively validate the target operating model before cutover.

Cross-domain infrastructure research reinforces the underlying systems logic. Nigerian evidence on integrating

decentralised solar infrastructure demonstrates that introducing autonomous technological capability into established operations requires coordination among technical, financial and governance conditions rather than isolated asset deployment (Sunday & Omoegun, 2018) [64]. Similarly, national-grid modelling shows that integration of new infrastructure is constrained by interoperability, data limitations and dependencies on existing systems (Shittu *et al*., 2019) [57]. These principles are transferable to corporate separation, where independent operation must be achieved without overlooking inherited interfaces.

Decentralised architectures further illustrate how autonomy can coexist with controlled interaction. Peer-to-peer microgrid research demonstrates that separately operating participants can transact through explicit rules, security mechanisms and defined interfaces instead of depending entirely on a central intermediary (Shittu *et al*., 2021) [60]. Applied cautiously to decoupling, this supports the architectural principle that separated entities should interact only through deliberately governed interfaces after trust boundaries have been redrawn.

The target environment must also reflect regional infrastructure realities. South African cloud-adoption research identifies technical expertise, connectivity, service-provider selection, data control and preparatory activities as important determinants of successful technology transition (Mudzamba, van der Schyff & Renaud, 2022) [49]. For a USD 1.5 million decoupling programme, these considerations translate into disciplined dependency discovery, target-state design, controlled coexistence, security-boundary reconfiguration, migration sequencing and final verification of service independence. Effective decoupling is therefore achieved not when systems are merely moved, but when each successor organisation can operate securely, support its business processes independently and demonstrate that residual technological dependencies are known, governed and progressively eliminated.

3. Pre-Separation Discovery, Dependency Mapping, and Infrastructure Baseline Assessment

Pre-separation discovery is the evidentiary foundation of secure IT decoupling because ownership cannot be transferred safely until the organisation understands what exists, where it resides, how it is configured, and what depends upon it. In post-transaction environments, inventories are often fragmented across configuration repositories, spreadsheets, vendor portals, cloud consoles and undocumented operational knowledge. A credible baseline should therefore identify configuration items, reconcile duplicate records and expose relationships among applications, servers, networks, databases, middleware, identities and business services. CMDB research demonstrates that automated discovery and dependency visualisation materially improve visibility across complex IT estates, particularly where configuration data originate from multiple repositories (Madduri *et al*., 2007) [43].

Discovery must proceed beyond asset enumeration to dependency mapping. Separation teams need to determine which components communicate, which services rely on common infrastructure, and which interfaces create hidden coupling between the divested and retained organisations. Configuration-management evidence shows that poorly planned CMDB initiatives can suffer from inappropriate levels of detail, weak maintenance and unrealistic expectations, making data quality and governance as important as tooling (Wu, 2014) [75]. Consequently, each discovered item should be linked to an owner, business process, criticality rating, technical location, lifecycle status and upstream or downstream dependency before migration scope is frozen.

The value of structured identification is reinforced by Nigerian RFID research, which demonstrates how unique tagging and automated capture can improve resource visibility, reduce manual errors and strengthen traceability (Yusuf *et al*., 2023) [77]. Although the study concerns library assets rather than enterprise infrastructure, the transferable principle is precise: separation decisions become more reliable when assets are uniquely identifiable and connected to authoritative records. For a corporate carve-out, equivalent discipline should encompass physical devices, virtual machines, software licences, certificates, service accounts and data stores.

Baseline assessment should also incorporate analytical prioritisation. A Nigerian supply-chain analytics framework illustrates how predictive, prescriptive and real-time analytics can reveal bottlenecks and support proactive decision-making across complex operating networks (Akin-Oluyomi & Akhigbe, 2023). Applied to IT separation, such analysis can identify highly connected applications, single points of failure, high-risk interfaces and services whose migration sequence could create disproportionate operational impact.

Cross-domain infrastructure research further illustrates the importance of mapping relationships before intervention. Hybrid solar optimisation demonstrates that distributed components must be evaluated as an interacting system because changes in allocation and control at one node affect overall performance (Sunday & Omoegun, 2019) [65]. Similarly, integrated AMR path-planning research shows that routing and resource placement cannot be optimised independently when congestion and operational dependencies interact dynamically (Akanbi & Sunday, 2024) [3]. These studies do not constitute IT-carve-out evidence, but they support the systems-engineering principle that decoupling requires relationship-aware analysis rather than isolated asset treatment.

Governance determines whether the resulting baseline can be trusted. Evidence from Ghanaian financial institutions shows that effective IT governance depends on coherent combinations of structures, processes and relational mechanisms rather than a single control instrument (Asmah & Kyobe, 2023) [14]. Accordingly, the pre-separation baseline should be formally validated by infrastructure, application, cybersecurity, finance, legal and business owners, with unresolved dependencies entered into a controlled risk register. For a USD 1.5 million decoupling programme, this baseline becomes the authoritative reference for scope, sequencing, cost estimation, cutover planning and post-separation verification, enabling programme leaders to distinguish genuinely independent services from assets that remain technically, commercially or operationally coupled in practice.

4. Separation Governance, Programme Management, and Stakeholder Accountability

Separation governance is the institutional mechanism through which a post-transaction IT decoupling programme

converts transaction objectives into controlled decisions, accountable workstreams, and measurable service-independence outcomes. Because infrastructure separation cuts across architecture, cybersecurity, applications, data, finance, legal obligations, vendors, and business operations, it should be governed as a coordinated programme rather than a collection of technical projects. M&A research shows that project, programme, and portfolio structures represent distinct modes of organising transaction-related change; for complex separations, a programme orientation is especially valuable because it integrates multiple interdependent projects while preserving strategic coherence (Geraldi, Teerikangas & Birollo, 2022) [27]. Accordingly, governance should establish an executive steering committee, a separation programme management office, named workstream leads, and explicit escalation routes before migration activity begins.

Effective governance also requires clearly defined decision rights. Ambiguity over who may approve architecture changes, security exceptions, expenditure, vendor commitments, data transfers, or cutover readiness can generate delay and unmanaged risk. Evidence from South African IT projects demonstrates that governance processes may exist formally yet remain ineffective when roles, procedures, communication, and enforcement are insufficiently defined (Mashiloane & Jokonya, 2018) [46]. In a decoupling programme, responsibility should therefore be documented through a decision-authority matrix covering the divestor, acquiring entity, internal technology teams, business owners, external vendors, cybersecurity personnel, and Transitional Service Agreement stakeholders.

Stakeholder accountability is equally important because separation decisions can redistribute cost, operational risk, and service responsibility across organisational boundaries. Project-governance scholarship emphasises that governance should define the roles and relationships of both internal and external stakeholders rather than focus narrowly on the project team (Derakhshan, Turner & Mancini, 2019) [20]. This implies maintaining a stakeholder register, issue and decision logs, risk ownership, dependency owners, and formal acceptance criteria for services moving into independent operation.

Governance must also ensure consistent compliance and quality across geographically distributed workstreams. Although developed for supply-chain networks, a Nigerian governance model demonstrates the transferable value of standardised policies, monitoring, accountability mechanisms, and performance feedback across dispersed operations (Akin-Oluyomi & Akhigbe, 2022) [9]. Within IT separation, common controls should therefore govern configuration changes, privileged access, migration evidence, testing, incident escalation, and documentation irrespective of site or platform.

Strategic alignment is another requirement. Technical teams may naturally optimise for system stability, while finance prioritises cost, legal teams focus on contractual exposure, and business leaders emphasise Day-1 continuity. Leadership research from Nigeria highlights the importance of connecting operational decisions with enterprise strategy through cross-functional coordination, data-driven oversight, and adaptive leadership (Akin-Oluyomi & Akhigbe, 2023). The separation PMO should translate these competing priorities into agreed milestones, risk tolerances, and decision criteria.

Transparency becomes particularly important in a USD 1.5 million programme, where expenditure must remain traceable to separation outcomes. Governance models for complex enterprises emphasise integrated reporting, digital dashboards, audit trails, accountability enforcement, and alignment between strategic objectives and execution (Akhigbe, Falemi & Akin-Oluyomi, 2025) [8]. Programme dashboards should therefore track budget consumption, critical-path milestones, unresolved dependencies, security exceptions, test completion, service readiness, and residual TSA exposure.

Finally, accountability should extend beyond delivery to benefits realisation. Leadership-performance research demonstrates the value of linking management actions to measurable operational outcomes through feedback mechanisms and performance indicators (Falemi, Akhigbe & Akin-Oluyomi, 2025) [25]. For secure decoupling, success should consequently be judged not only by completion dates and expenditure, but by verified service autonomy, removal of inappropriate access, closure of shared dependencies, stable post-cutover operations, and formal acceptance by accountable business and technology owners. This governance discipline also strengthens auditability throughout ownership transition and stabilisation.

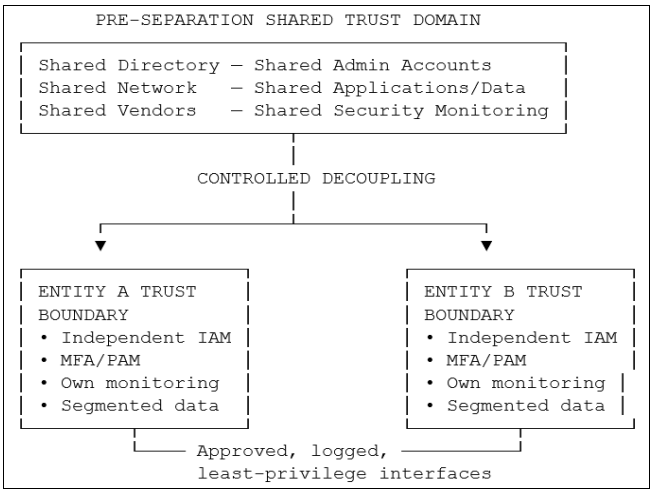
5. Identity, Access, Cybersecurity, and Trust Boundary Reconfiguration

Identity and access reconfiguration is among the most security-critical workstreams in IT decoupling because ownership transition alters who is legitimately entitled to access systems, data and administrative functions. During separation, inherited directories, federated identities, shared credentials, service accounts and privileged roles may remain connected to both successor environments, creating opportunities for unauthorised persistence or lateral movement. Zero Trust provides an appropriate architectural principle by removing implicit confidence based on network location and requiring explicit authentication and authorisation for access to protected resources (Rose *et al*., 2020) [54].

The immediate objective should be to establish authoritative identity ownership. Employee, contractor, vendor, application and machine identities must be classified according to the entity that will control them after separation, while dormant and duplicate accounts should be eliminated. Multi-factor authentication is especially important during transitional periods because compromised passwords can otherwise provide access across overlapping environments; combining independent authentication factors materially strengthens assurance compared with password-only mechanisms (Ometov *et al*., 2018) [51]. Identity cutover should therefore be sequenced alongside HR transfer dates, application migration and contractual access requirements.

Privileged identities require stronger treatment because administrative accounts can alter infrastructure, modify security policies and create new access pathways. Financial-sector Zero Trust research emphasises identity and access management, device security and data protection as interdependent implementation domains rather than isolated controls (Daah, Qureshi & Awan, 2023) [19]. Accordingly, privileged accounts inherited from the former owner should be inventoried, reassigned where necessary, rotated at cutover, subjected to time-bound elevation and monitored until legacy connectivity is removed.

Fine-grained authorisation becomes equally important where systems must remain temporarily interconnected. Attribute-based controls can incorporate role, organisational affiliation, resource sensitivity and operational context into access decisions instead of relying exclusively on broad static groups. Although developed for supply-chain information exchange, attribute-based encryption research demonstrates how data access can be restricted according to explicit attributes even within distributed environments (Shittu & Nabil, 2023) [56]. In a decoupling programme, this principle is applicable to temporary vendor, migration-team, and Transitional Service Agreement access.



Source: Author-developed conceptual figure.

Fig 1: Illustrative trust-boundary reconfiguration during IT services decoupling

Network trust boundaries must be redrawn simultaneously with identity boundaries. Comprehensive Zero Trust scholarship identifies micro-segmentation, continuous verification and policy enforcement as mechanisms for preventing a compromise in one security zone from automatically propagating into another (Syed *et al*., 2022) [67]. Consequently, transitional network routes should be treated as explicit exceptions with owners, expiry dates and traffic restrictions rather than extensions of the former corporate perimeter.

Cloud and remote-access environments introduce additional complexity because access may originate outside traditional infrastructure. Dynamic Zero Trust policy research demonstrates how access decisions can incorporate contextual conditions and be adjusted as environments change, supporting temporary but controlled access during distributed operations (Mandal, Khan & Jain, 2021) [45]. For separation programmes, this supports conditional access based on device posture, user identity, location and resource sensitivity.

Cybersecurity controls must also reflect regional operational realities. Nigerian banking research documents material exposure to cyber breaches and uneven security capability in digitally enabled financial services, demonstrating why transition periods should not rely on informal trust relationships or inherited credentials (Wang, Nnaji & Jung, 2020) [73]. South African cyber-banking research similarly highlights vulnerabilities arising from interconnected network and application environments, reinforcing the importance of defensible security boundaries when ownership changes (Mbah Mbelli & Dwolatzky, 2016) [47].

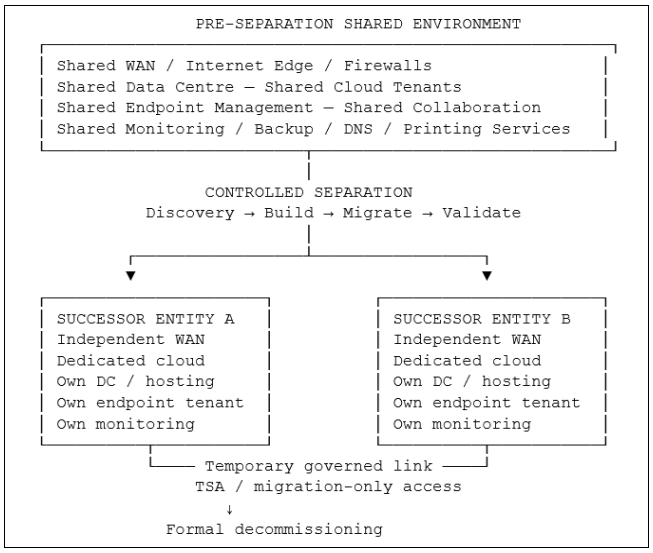
Finally, trust-boundary reconstruction must be validated rather than assumed. Critical analysis of Zero Trust emphasises that architecture effectiveness depends on coherent policy decisions, enforcement and resource-protection mechanisms rather than simply deploying additional security products (Fernandez & Brazhuk, 2024) [26]. For a USD 1.5 million decoupling programme, completion criteria should therefore include independent identity stores, credential rotation, privileged-access segregation, revoked legacy accounts, segmented connectivity, complete audit logging and formal verification that neither successor organisation retains unauthorised access to the other's infrastructure. These controls transform legal ownership separation into demonstrable technical and cybersecurity independence.

6. Network, Cloud, Data Centre, and End-User Infrastructure Separation

Infrastructure separation is the point at which a transaction becomes operationally tangible. Networks, cloud tenancies, data-centre platforms, endpoints, and local services that were previously engineered as a common environment must be reorganised so that each successor organisation can function independently without introducing unacceptable downtime, security gaps, or performance degradation. Enterprise cloud-migration research shows that apparently straightforward moves from an internal data centre to infrastructure-as-a-service can create organisational and technical consequences extending well beyond hosting cost, making stakeholder impact and service-dependency assessment essential before execution (Khajeh-Hosseini, Greenwood & Sommerville, 2010) [38].

A defensible separation strategy should begin with target-state architecture and migration classification. Workloads should be designated for relocation, replication, retirement, retention under temporary shared service, or re-platforming according to business criticality, technical compatibility, latency requirements, and recovery objectives. Reviews of cloud-migration processes demonstrate that successful transitions require structured assessment, planning, execution, and evaluation activities rather than ad hoc workload movement (Gholami *et al*., 2016) [28]. This logic is particularly important in a USD 1.5 million decoupling programme, where uncontrolled redesign can consume budget without producing genuine service independence.

Network separation requires more than changing IP ranges or firewall rules. Routing, DNS, load balancing, WAN connectivity, VPNs, wireless services, and network-management platforms may contain hidden dependencies between retained and separated entities. Network virtualisation and software-defined networking provide mechanisms for abstracting logical connectivity from physical infrastructure, thereby enabling programmable, policy-driven reconfiguration while reducing dependence on fixed hardware topology (Jain & Paul, 2013) [35]. During decoupling, temporary inter-entity routes should therefore be explicitly documented, secured, monitored, and assigned expiry dates.



Source: Author-developed conceptual figure.

Fig 2: Illustrative infrastructure separation architecture

Cloud and virtualised data-centre workloads should be migrated in waves reflecting technical dependency and service-level commitments. Research on SDN-NFV-enabled environments shows that concurrent migrations can affect bandwidth, execution time, downtime, and quality of service, making sequencing and scheduling central to continuity management (He, Toosi & Buyya, 2021) [30]. High-criticality services should therefore be rehearsed, rollback-capable, and migrated within controlled windows, while lower-risk infrastructure can validate tooling and operational procedures before larger waves proceed.

African operating conditions further reinforce readiness-based sequencing. Research involving large South African enterprises demonstrates that cloud maturity depends on organisational scale, executive support, infrastructure capability, security concerns, and the balance between efficiency and agility (Moonasar & Naicker, 2020) [48]. Separation plans should consequently avoid assuming uniform readiness across locations; offices and remote facilities may require differentiated connectivity, redundancy, caching, and support arrangements.

Physical infrastructure remains relevant even where separation is predominantly cloud-led. Nigerian engineering research on medium-voltage networks shows, by analogy, that resilient distributed infrastructure depends upon site-specific assessment, protection, monitoring, and lifecycle planning rather than standardised deployment alone (Adeniji *et al*., 2020) [2]. For IT decoupling, racks, power, cabling, network appliances, and local compute should similarly be mapped to ownership, capacity, resilience, and failover requirements before shared facilities are decommissioned.

Automation can reduce configuration drift during large-scale separation. The supplied Siemens TIA Portal study illustrates the transferable value of unified engineering environments for synchronising configuration, monitoring, and control across interconnected systems (Sunday & Omoegun, 2022) [66]. In enterprise IT, infrastructure-as-code, automated provisioning, and standard build templates can similarly improve repeatability, although the cited work remains an industrial-automation analogue rather than direct evidence on corporate infrastructure separation.

Observability must remain active throughout cutover. SCADA research demonstrates how integrated monitoring, analytics, and automation can enhance operational visibility and rapid response across distributed environments (Omoegun *et al*., 2024) [53]. For separated IT estates, equivalent discipline requires centralised logging, endpoint monitoring, capacity dashboards, and incident escalation so that failures introduced during migration are identified before they propagate across services.

End-user separation should likewise be treated as an infrastructure workstream rather than an afterthought. Devices must be reassigned to the correct management tenant, rebuilt where necessary, re-enrolled into endpoint protection, connected to new printing and collaboration services, and tested against required applications. Cross-domain research on grid automation similarly illustrates the value of real-time management and resilient control when complex infrastructure is being reconfigured (Shittu, Adaramola & Shittu, 2025) [61]. The architecture represented in Fig 2 therefore places end-user services alongside network, cloud, and data-centre layers, with controlled coexistence maintained only until validation confirms operational autonomy.

7. Application, Data, Integration, and Information-Ownership Decoupling

Application, data, integration, and information-ownership decoupling constitutes one of the most consequential stages of post-transaction IT separation because business continuity depends on preserving required information flows while eliminating inappropriate technological and legal dependencies. Applications should therefore be classified according to future ownership, business criticality, interface dependency, data sensitivity, and disposition strategy—retain, migrate, replicate, replace, archive, or retire. Post-merger information-systems research demonstrates that integration risk arises from interacting technical and organisational conditions, requiring explicit treatment of dependencies, timing, and business process continuity rather than isolated system decisions (Alaranta & Mathiassen, 2014).

Application disentanglement should be driven by target-state capability rather than by simple asset transfer. Where two entities share ERP modules, middleware, APIs, reporting tools, or bespoke applications, separation teams must determine which interfaces can be terminated, which require temporary coexistence, and which must be rebuilt under independent ownership. Decision-support research for post-merger information systems shows that integration choices should reflect business strategy, existing system characteristics, and the desired future architecture, providing a defensible basis for application-level disposition decisions (Lace, 2023).

Data separation requires equally rigorous governance. Customer, employee, supplier, financial, operational, and regulatory datasets should be assigned authoritative owners, mapped to lawful purposes, reconciled across duplicate repositories, and subjected to quality controls before migration. Financial-sector data-governance research emphasises clearly defined roles, metadata management, data-quality accountability, and governance processes as foundations for reliable information management (Karkošková, 2023).

In Nigeria, ownership transition also carries statutory implications because personal information cannot be treated as an unrestricted transferable asset. The Nigerian data-

protection framework establishes institutional and legal responsibilities around processing, accountability, and protection of personal data, making lawful control, retention, and access central considerations when datasets move between corporate entities (Babalola, 2022).

Across Africa, financial digitalisation further increases the importance of data sovereignty, cross-border governance, interoperability, and institutional capacity. African financial-data research shows that expanding digital ecosystems require governance arrangements capable of balancing innovation, inclusion, privacy, and regulatory control, particularly where information traverses organisational and national boundaries (Ndemo & Mkalama, 2023).

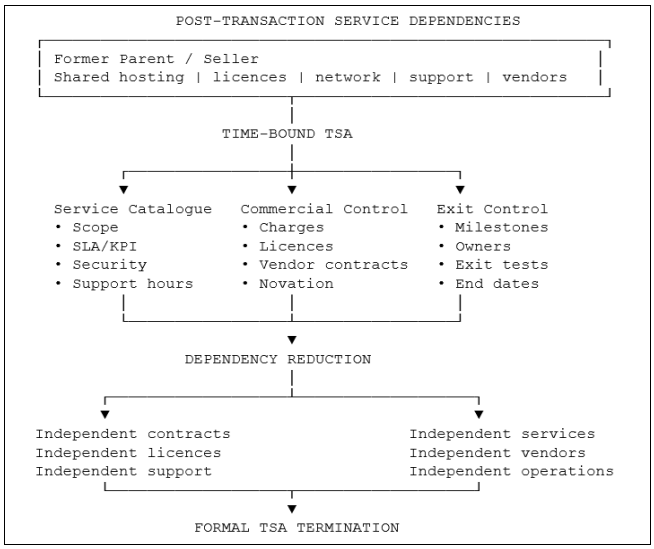
Secure exchange mechanisms are therefore necessary during temporary coexistence. Although derived from SCADA environments, blockchain-assisted architecture research demonstrates the transferable value of integrity verification, controlled access, auditability, and tamper-resistant exchange across distributed systems (Shittu *et al*., 2022). For a USD 1.5 million decoupling programme, these principles support controlled interface migration, reconciled data transfer, documented ownership, validated records, and decommissioning of connections once independent application and information domains have been demonstrably established.

8. Transitional Service Agreements, Vendors, Licensing, and Commercial Dependencies

Transitional Service Agreements (TSAs) are central to post-transaction IT separation because they provide temporary continuity where the acquiring or separated entity cannot assume full operational control on legal close. Their value lies in preserving essential services while independent infrastructure, applications, contracts and support capabilities are established. However, a TSA should function as an exit mechanism rather than a substitute operating model. Contract research on IT outsourcing shows that flexible arrangements and explicit rights to terminate, reconfigure or bring services back in-house reduce the risk that temporary dependence becomes structurally embedded (Benaroch, Dai & Kauffman, 2010).

Commercial dependency is especially acute where software licences, cloud subscriptions, maintenance agreements or managed-service contracts were negotiated at group level. During separation, entitlement may not automatically transfer with the business unit, and pricing may change once enterprise-wide volume discounts disappear. Research on asset transfer in IT outsourcing demonstrates that contractual design must address ownership, incentives, pricing and protective clauses when technology assets move between organisational boundaries (Chang, Gurbaxani & Ravindran, 2017). Accordingly, separation inventories should distinguish transferable licences, non-transferable rights, novation requirements, termination costs and replacement procurement.

Vendor lock-in creates a related risk. Proprietary data formats, APIs and platform-specific services can make migration technically difficult and commercially expensive. Evidence from cloud computing shows that interoperability, portability, data ownership and contract-exit provisions are critical mechanisms for reducing dependence on a single provider (Opara-Martins, Sahandi & Tian, 2016). TSA design should therefore specify data-return formats, migration assistance, documentation obligations and firm exit dates.



Source: Author-developed conceptual figure.

Fig 3: Illustrative TSA and Commercial Dependency Exit Framework

Cybersecurity obligations must also survive commercial transition. Outsourcing contracts increasingly require explicit allocation of security responsibilities, audit rights, subcontractor controls, incident notification and tested exit arrangements, particularly for regulated organisations (Bomhard & Daum, 2021). This is important where a divested entity continues to consume identity, hosting, monitoring or network services from its former owner during a limited coexistence period.

Vendor capability should be treated as a risk variable rather than assumed from contract award. South African evidence identifies service-provider risk profiling, audit, assurance and governance as necessary disciplines for managing external IT dependencies (Badru, Ajayi & Ndayizigamiye, 2023). These controls support periodic TSA reviews against service levels, unresolved dependencies and exit readiness.

The Nigerian context similarly demonstrates that software outsourcing decisions are affected by technical capability, commercial conditions, legal considerations and confidence in supplier maturity (Casado-Lumbreras *et al*., 2014). For a geographically distributed separation, vendor due diligence should therefore include financial resilience, local support capacity, licensing authority, security capability and transition assistance.

Finally, in practice, commercial decoupling depends on relationship governance as much as legal drafting. Contemporary outsourcing research shows that trust, information exchange, coordination and adaptive governance shape client-vendor performance over time (Ngah, Tjemkes & Dekker, 2024). For a USD 1.5 million decoupling programme, TSA governance should combine service-level dashboards, named dependency owners, cost transparency, licence-transition plans and milestone-based exit gates so that every temporary commercial dependency has an accountable owner, measurable duration and defined path to termination or independent replacement.

9. Migration Execution, Cutover Management, Testing, and Operational Continuity

Migration execution is the phase in which separation design is converted into operational reality, and its discipline determines whether independent services remain secure, available and usable after ownership transition. Execution should be organised into controlled migration waves based on service criticality, technical dependency, recovery objectives and business tolerance for interruption. Because distributed transitions require specialised knowledge across infrastructure, applications, cybersecurity and user support, capability development should precede cutover; structured competency building strengthens workforce adaptability across dispersed operations (Falemi, Akhigbe & Akin-Oluyomi, 2020) [22].

Cutover planning should translate each migration wave into a time-bound runbook specifying prerequisites, responsible owners, sequencing, communication channels, decision gates, contingency actions and rollback criteria. Staffing must reflect the intensity of transition windows, particularly where overnight activities extend across multiple sites and technical teams. Workforce-centred operational research shows that skill heterogeneity, fatigue and shift variability influence throughput and system stability, supporting deliberate allocation of experienced personnel across critical cutover tasks rather than uniform staffing assumptions (Akanbi, Ganiu & Sunday, 2022) [5].

Testing should be layered rather than confined to a final technical check. Infrastructure connectivity, authentication, interfaces, data reconciliation, security controls, end-user functionality and business processes should be validated before service acceptance. Real-time operational information is useful during this period because performance deviations can be identified rapidly and linked to frontline behaviour or process conditions, helping transition teams preserve customer-facing service quality while corrective actions are undertaken (Akhigbe, Falemi & Akin-Oluyomi, 2023) [7].

Operational continuity also requires capacity to absorb unexpected workload. Separation programmes experience clustered incidents after migrations as users encounter configuration differences, missing permissions or exposed dependencies. Predictive staffing and flexible resource allocation can align support capacity with fluctuating operational demand, reducing the risk that incident backlogs compromise stabilisation or prolong dependence on the former owner (Falemi, Akhigbe & Akin-Oluyomi, 2023b) [24].

Hypercare should therefore be treated as a controlled extension of cutover rather than informal post-project support. Specialists should remain available while incident trends, service performance, security alerts and unresolved defects are monitored against predefined exit thresholds. Retaining knowledgeable personnel during this interval is important because workforce stability and operational productivity are interrelated; loss of critical knowledge can weaken response capability when the new environment requires rapid diagnosis and remediation (Falemi, Akhigbe & Akin-Oluyomi, 2023a) [23].

Human factors should also inform execution governance. High-pressure cutovers involve sustained attention, rapid judgement and coordination across technical and business teams. A multimodal cognitive-workload framework indicates that physiological, behavioural and subjective indicators can provide complementary perspectives on operator workload, suggesting that complex transitions should avoid excessive task concentration, prolonged shifts and decision overload that may increase error exposure (Adamolekun *et al*., 2025) [1].

For a USD 1.5 million decoupling programme, operational acceptance should be evidence-based: successful completion requires validated service availability, functioning recovery arrangements, reconciled data, effective access controls, closed defects, rollback outcomes and documented business-owner acceptance. South African evidence associates stronger IT controls with more effective organisational control environments, reinforcing the importance of change management, backup, recovery and continuity controls throughout migration rather than after separation has occurred (Lebese & Motubatse, 2025) [41].

10. Performance Evaluation and Lessons from a USD 1.5 Million IT Decoupling Programme

Performance evaluation in an IT decoupling programme should extend beyond whether migration activities were completed on time and within the approved USD 1.5 million budget. A separation initiative succeeds only when the successor environment operates independently, securely and reliably, while users, applications and business processes continue to function at an acceptable level. Research on IT project success demonstrates that formal definitions of success improve evaluation quality because organisational benefits, stakeholder expectations and technical outcomes must complement the conventional measures of cost, schedule and scope (Thomas & Fernández, 2008) [70]. For this programme, evaluation should therefore combine financial control with evidence of service autonomy, operational stability, security assurance and business acceptance.

Cost and schedule performance remain important because they reveal whether resources were converted into deliverables efficiently. Evidence from a large portfolio of information-systems projects in the banking sector shows that project size, duration, team allocation and managerial authority materially influence cost-and-time performance (Sanchez, Terlizzi & Moraes, 2017) [55]. Applied to the decoupling programme, budget variance, milestone adherence, change-request volume, resource utilisation and vendor expenditure should be reviewed against the approved baseline. These measures can identify where complexity, underestimated dependencies or execution delays consumed disproportionate programme capacity without assuming that budget compliance alone constitutes success.

Performance must also be evaluated across sites rather than solely at programme level. A Nigerian multi-site performance framework emphasises integrated indicators, real-time analytics and cross-location comparison as mechanisms for identifying bottlenecks and uneven operational outcomes (Akin-Oluyomi & Akhigbe, 2023). Accordingly, branch, data-centre, cloud and end-user environments should be assessed using common indicators such as service availability, incident rates, access failures, migration defects, unresolved dependencies and support volumes. This prevents strong aggregate results from concealing weak performance within individual locations.

Post-cutover reliability is another critical dimension. Condition-monitoring research from Nigeria demonstrates the value of continuous observation and trend analysis for

detecting abnormal system behaviour before it develops into significant operational failure (Omoegun *et al*., 2023) [52]. Translated to IT separation, monitoring should track infrastructure health, latency, authentication errors, application failures, backup status and security events during stabilisation. Such evidence allows programme teams to distinguish temporary migration noise from persistent architectural defects.

Continuous improvement should be embedded in the evaluation cycle. Lean Six Sigma and reliability-centred maintenance research argues for combining process-variation reduction with reliability analysis so that performance improvement addresses both efficiency and recurrent failure (Olutimehin & Ganiu, 2022) [50]. In a decoupling context, incident trends, failed change records, rollback events and recurring support tickets should feed root-cause reviews and corrective-action plans. Lessons identified during one migration wave should therefore inform subsequent cutovers and final decommissioning activities.

Evaluation should also recognise that project success changes over time. South African information-systems research distinguishes short-, medium- and long-term dimensions of success and shows that different stakeholders may judge outcomes differently depending on when benefits are assessed (Joseph & Marnewick, 2021) [37]. Immediate measures may emphasise cutover stability and user access, whereas later assessment should consider reduction of transitional-service dependence, security posture, operating cost and sustained service quality.

The central lesson for a USD 1.5 million decoupling programme is that measurement must remain aligned with the strategic purpose of separation. Performance-management research shows that project indicators create value when they connect project execution with wider organisational success rather than becoming isolated reporting exercises (Korhonen *et al*., 2023) [39]. Accordingly, the programme scorecard should combine financial, operational, security, user and dependency-exit measures, supported by documented baselines and accountable owners. This approach enables lessons from migration defects, vendor performance, architectural constraints and stakeholder experience to be converted into reusable knowledge for future mergers, acquisitions, divestitures and ownership transitions across complex geographically distributed enterprise environments.

11. Secure Decoupling Framework, Strategic Priorities, and Future Research Directions

A secure decoupling framework should convert the lessons of post-transaction separation into a repeatable lifecycle rather than treat each ownership transition as an isolated exercise. The framework should begin with dependency discovery, proceed through target-state design, trust-boundary reconstruction, controlled migration and validation, and end with formal decommissioning and benefits assurance. Each stage should have measurable entry and exit criteria covering asset ownership, identity separation, data control, connectivity, service continuity, commercial dependencies and residual risk. Digital-twin research in Nigerian smart substations demonstrates the value of continuously updated virtual representations for monitoring complex assets and identifying faults before disruption; translated cautiously to enterprise separation, this suggests that future programmes could use digital replicas of application, network and infrastructure dependencies to rehearse cutovers and test failure scenarios before production change (Shittu *et al*., 2023) [62].

Cybersecurity must remain embedded throughout the lifecycle rather than be positioned as a final assurance activity. Ownership transitions create temporary interfaces, duplicated control planes and residual privileges that can undermine otherwise successful migration. Research on cyber-physical resilience shows that adaptive protection, real-time telemetry and coordinated response can strengthen interconnected systems under changing conditions (Shittu, Olagunju & Shittu, 2024) [59]. For secure decoupling, the corresponding priority is continuous assurance: temporary connections should be monitored, exceptions time-bounded, privileged access recertified, and separation milestones linked to security evidence rather than completion declarations alone.

A second priority is predictive transition management. AI-enabled digital twins can combine live telemetry, historical behaviour and simulation to anticipate abnormal operating conditions and support optimisation decisions (Shittu & Shittu, 2024) [58]. In future IT separation programmes, similar techniques could model workload movement, forecast capacity stress, identify emerging dependency failures and compare alternative migration sequences. Their use should nevertheless be constrained by data quality, explainability, model drift and governance requirements where automated recommendations affect regulated systems. The verified publication describes a cloud-edge digital-twin architecture combining real-time data with AI-based analysis, illustrating the underlying transferable capability.

Observability and distributed control also require greater attention. IoT-enabled integration research illustrates how heterogeneous devices, storage resources and management platforms can be coordinated through common supervisory architectures while maintaining resilience across distributed environments (Shittu *et al*., 2025) [63]. Within decoupling, this principle supports unified telemetry across cloud, data-centre, endpoint and network layers during coexistence. Future architectures should therefore emphasise vendor-neutral observability, portable configuration data and standardised interfaces so separation teams can monitor the transition without creating a new dependency on a single platform.

Autonomous coordination represents a further research frontier. Multi-agent AI models show how decentralised agents can distribute decision-making across complex operational environments rather than depend entirely on a single controller (Akanbi, Ganiu & Sunday, 2025) [6]. Although this literature is not concerned with M&A separation, the concept is relevant to future orchestration research: specialised agents could potentially supervise identity migration, application readiness, network dependencies, testing evidence and incident escalation under human-defined controls. Research should examine whether such approaches improve speed and consistency without creating opaque decision chains or unacceptable automation risk.

The wider AMR literature also highlights scalability, interoperability and dynamic coordination when autonomous systems operate across changing environments (Akanbi & Sunday, 2025) [4]. For secure IT decoupling,

these themes point toward reusable automation patterns for discovery, migration sequencing, dependency validation and post-cutover verification. Future studies should compare total transition cost, user disruption, service availability, security incidents, TSA duration and stranded-asset reduction across manual, automated and AI-assisted separation models.

Finally, strategic maturity requires institutional learning. Evidence from South Africa's Transnet case shows that cyber resilience is shaped not only by technical controls but also by governance, investment priorities and organisational accountability for critical digital infrastructure (Timcke, Gaffley & Rens, 2023) [71]. This is especially relevant to African and other emerging-market contexts, where research should investigate how regulatory maturity, infrastructure quality, skills availability and vendor concentration influence decoupling outcomes. Building on the USD 1.5 million programme, future work should develop comparative maturity models, benchmark separation costs, test digital-twin-assisted cutovers, quantify residual dependency risk and examine how governance choices affect long-term service independence. Such evidence would transform secure decoupling from transaction-specific practice into a measurable enterprise capability.

12. Conclusion

This study examined the strategic, technical, operational, and governance requirements for securely separating IT services following mergers, acquisitions, divestitures, and ownership transitions. The review met its aims by establishing the conceptual basis of decoupling, identifying the risks embedded in transitional environments, evaluating the controls required for infrastructure and information separation, and developing a practical framework informed by lessons from a USD 1.5 million decoupling programme.

The findings demonstrate that successful separation is not achieved through asset transfer alone. Effective decoupling requires accurate discovery, dependency mapping, infrastructure baselining, disciplined governance, explicit accountability, identity and trust-boundary reconfiguration, controlled network and cloud separation, application and data disentanglement, and structured management of Transitional Service Agreements, licensing, vendors, and residual commercial dependencies. Migration execution must be supported by rigorous testing, cutover governance, rollback capability, workforce readiness, hypercare, and measurable operational acceptance. Performance evaluation further showed that cost and schedule metrics are insufficient unless accompanied by evidence of service autonomy, security assurance, reduced dependency, user stability, and sustained business continuity.

The study also found that emerging capabilities, including digital twins, AI-enabled analytics, automated orchestration, real-time observability, and resilient distributed architectures, can strengthen future separation programmes when governed carefully and aligned with organisational maturity. The applied lessons indicate that decoupling should be treated as a lifecycle capability rather than a one-off technical project.

Accordingly, organisations should institutionalise separation playbooks, maintain authoritative asset and dependency inventories, strengthen identity governance, define measurable TSA exit criteria, embed cybersecurity throughout transition, and link programme dashboards to business outcomes. Future research should develop comparative maturity models, quantify residual dependency risk, evaluate automation-assisted cutovers, and examine how regulatory conditions, workforce capability, infrastructure quality, and vendor concentration influence outcomes across sectors and emerging-market environments. Longitudinal studies should also assess whether separation benefits persist after TSA termination, particularly regarding operating cost, cyber resilience, service performance, governance effectiveness, and sustained strategic technology independence.

13. References

1. Adamolekun A, Logah FX, Alabi C, Baanye J, Wilson M, Ganiu O, *et al*. Toward a unified framework for multimodal cognitive workload assessment in human-machine interaction systems. SSRN Electronic Journal, 2025. Doi: https://doi.org/10.2139/ssrn.5235980 (SSRN)
2. Adeniji IO, Shittu H, Elumilade RA, Opara IS, Shittu MA. Grounding system design optimization for medium-voltage distribution networks in emerging power markets. Iconic Research and Engineering Journals. 2020; 3(11):547-565. Doi: https://doi.org/10.64388/IREV3I11-1714040. (IRE Journals)
3. Akanbi O, Sunday EA. An integrated path-planning and slotting optimization model for AMR-enabled high-density warehousing. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):3226-3243. Doi: https://doi.org/10.62225/2583049X.2024.4.6.6181. (Multiresearch Journal)
4. Akanbi O, Sunday EA. A systematic review of AI-driven autonomous mobile robots (AMR) in scalable micro-fulfillment centers. International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(6):2363-2379. Doi: https://doi.org/10.62225/2583049X.2025.5.6.6182
5. Akanbi O, Ganiu OS, Sunday EA. A workforce-centric line-balancing model for throughput maximization in multi-shift operations. Shodhshauryam: International Scientific Refereed Research Journal. 2022; 5(3):439-464. Publisher-listed Doi: https://doi.org/10.32628/SHISRRJ. (ResearchGate)
6. Akanbi O, Ganiu OS, Sunday EA. A multi-agent AI framework for swarm intelligence in autonomous mobile robot (AMR) fleet coordination. International Journal of Scientific Research in Humanities and Social Sciences. 2025; 2(1):81-109. Publisher-listed Doi: https://doi.org/10.32628/IJSRHSS
7. Akhigbe R, Falemi A, Akin-Oluyomi OT. A conceptual model for improving customer experience using workforce behavior and real-time operational data. International Journal of Multidisciplinary Research and Growth Evaluation. 2023; 4(6):1322-1338. Doi: https://doi.org/10.54660/.IJMRGE.2023.4.6.1322-1338. (All Multidisciplinary Journal)
8. Akhigbe R, Falemi A, Akin-Oluyomi OT. An advanced governance model for improving transparency, accountability and strategic execution in complex enterprises. International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(6):1169-1188. Doi:

https://doi.org/10.62225/2583049X.2025.5.6.5341. (Multiresearch Journal)
9. Akin-Oluyomi OT, Akhigbe R. A supply chain governance model for enhancing compliance and operational quality across retail networks. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(6):860-878. Doi: https://doi.org/10.54660/.IJMRGE.2022.3.6.860-878. (All Multidisciplinary Journal)
10. Akin-Oluyomi OT, Akhigbe R. A conceptual supply chain leadership model for aligning logistics decisions with enterprise strategy. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(1):1725-1744. Doi: https://doi.org/10.62225/2583049X.2023.3.1.5340. (Multiresearch Journal)
11. Akin-Oluyomi OT, Akhigbe R. A proposed supply chain analytics framework for improving forecasting accuracy and reducing bottlenecks. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(1):1686-1703. Doi: https://doi.org/10.62225/2583049X.2023.3.1.5338. (Multiresearch Journal)
12. Akin-Oluyomi OT, Akhigbe R. An advanced framework for improving multi-site operational efficiency using data-driven performance indicators. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(1):1763-1781. Doi: https://doi.org/10.62225/2583049X.2023.3.1.5343. (Multiresearch Journal)
13. Anderson-Princen JM. 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. European Business Organization Law Review. 2022; 23(4):905-936. Doi: https://doi.org/10.1007/s40804-022-00252-4. (Springer)
14. Asmah A, Kyobe M. A configurational analysis of IT governance: A study of the financial services sector in Ghana. The Electronic Journal of Information Systems in Developing Countries. 2023; 89(1):e12237. Doi: https://doi.org/10.1002/isd2.12237. (Wiley Online Library)
15. Ayagre P, Aboagye AQQ, Sarpong-Kumankoma E, Asuming PO. Bank mergers and acquisitions and the post-merger and acquisition performance of combined banks: Evidence from Sub-Saharan Africa. Cogent Economics & Finance. 2024; 12(1):2319167. Doi: https://doi.org/10.1080/23322039.2024.2319167. (Taylor & Francis Online)
16. Blatman P, Lukac E. The role of IT in mergers and acquisitions. In Roehl-Anderson, J.M. (ed.) M&A Information Technology Best Practices. Hoboken, NJ: Wiley, 2013, 23-34. Doi: https://doi.org/10.1002/9781118692028.ch2
17. Boadi I, Mawutor JKM, Dzorka MA, Kubaje TA. The productivity paradox of information technology: The Ghanaian bank-level evidence. The Electronic Journal of Information Systems in Developing Countries. 2022; 88(4):e12211. Doi: https://doi.org/10.1002/isd2.12211. (Wiley Online Library)
18. Chang S-I, Chang I-C, Wang T. Information systems integration after merger and acquisition. Industrial Management & Data Systems. 2014; 114(1):37-52. Doi: https://doi.org/10.1108/IMDS-03-2013-0157
19. Daah C, Qureshi A, Awan I. Zero Trust Model Implementation Considerations in Financial Institutions: A Proposed Framework. In 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2023, 71-77. Doi: https://doi.org/10.1109/FiCloud58648.2023.00019
20. Derakhshan R, Turner R, Mancini M. Project governance and stakeholders: A literature review. International Journal of Project Management. 2019; 37(1):98-116. Doi: https://doi.org/10.1016/j.ijproman.2018.10.007. (ScienceDirect)
21. Fähling J, Leimeister JM, Yetton P, Krcmar H. Managing an IT carve-out at a multi-national enterprise. Journal of Information Technology Teaching Cases. 2013; 3(2):106-110. Doi: https://doi.org/10.1057/jittc.2013.10. (Sage Journals)
22. Falemi A, Akhigbe R, Akin-Oluyomi OT. A conceptual supply chain talent development model for capability building across distributed operations. International Journal of Multidisciplinary Research and Growth Evaluation. 2020; 1(5):439-456. Doi: https://doi.org/10.54660/.IJMRGE.2020.1.5.439-456. (All Multidisciplinary Journal)
23. Falemi A, Akhigbe R, Akin-Oluyomi OT. A proposed framework for integrating employee retention systems with operational productivity metrics. International Journal of Advanced Multidisciplinary Research and Studies. 2023a; 3(1):1704-1724. Doi: https://doi.org/10.62225/2583049X.2023.3.1.5339. (Multiresearch Journal)
24. Falemi A, Akhigbe R, Akin-Oluyomi OT. A supply chain workforce optimization framework for addressing staffing volatility during rapid expansion cycles. International Journal of Advanced Multidisciplinary Research and Studies. 2023b; 3(1):1745-1762. Doi: https://doi.org/10.62225/2583049X.2023.3.1.5342. (Multiresearch Journal)
25. Falemi A, Akhigbe R, Akin-Oluyomi OT. A proposed operational growth framework linking leadership effectiveness with measurable business outcomes. International Journal of Multidisciplinary Research and Growth Evaluation. 2025; 6(6):1081-1102. Doi: https://doi.org/10.54660/.IJMRGE.2025.6.6.1081-1102. (All Multidisciplinary Journal)
26. Fernandez EB, Brazhuk A. A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces. 2024; 89:103832. Doi: https://doi.org/10.1016/j.csi.2024.103832. (Springer Link)
27. Geraldi J, Teerikangas S, Birollo G. Project, program and portfolio management as modes of organizing: Theorising at the intersection between mergers and acquisitions and project studies. International Journal of Project Management. 2022; 40(4):439-453. Doi: https://doi.org/10.1016/j.ijproman.2022.03.005. (ScienceDirect)
28. Gholami MF, Daneshgar F, Low G, Beydoun G. Cloud migration process-A survey, evaluation framework, and open challenges. Journal of Systems and Software. 2016; 120:31-69. Doi: https://doi.org/10.1016/j.jss.2016.06.068. (VU Repository)
29. Gomes E, Angwin D, Peter E, Mellahi K. HRM issues

and outcomes in African mergers and acquisitions: A study of the Nigerian banking sector. The International Journal of Human Resource Management. 2012; 23(14):2874-2900. Doi: https://doi.org/10.1080/09585192.2012.671509. (Taylor & Francis Online)
30. He T, Toosi AN, Buyya R. SLA-aware multiple migration planning and scheduling in SDN-NFV-enabled clouds. Journal of Systems and Software. 2021; 176:110943. Doi: https://doi.org/10.1016/j.jss.2021.110943. (ScienceDirect)
31. Henningsson S, Carlsson S. The DySIIM model for managing IS integration in mergers and acquisitions. Information Systems Journal. 2011; 21(5):441-476. Doi: https://doi.org/10.1111/j.1365-2575.2011.00374.x. (Wiley Online Library)
32. Henningsson S, Kettinger WJ. Understanding information systems integration deficiencies in mergers and acquisitions: A configurational perspective. Journal of Management Information Systems. 2016; 33(4):942-977. Doi: https://doi.org/10.1080/07421222.2016.1267516. (JMIS)
33. Henningsson S, Øhrgaard C. Acquisition IT integration: The roles of temporary agency workers. In ECIS 2015 Proceedings, Article 76. Association for Information Systems, 2015. Doi: https://doi.org/10.18151/7217354. (CBS Research Portal)
34. Henningsson S, Yetton PW, Wynne PJ. A review of information system integration in mergers and acquisitions. Journal of Information Technology. 2018; 33(4):255-303. Doi: https://doi.org/10.1057/s41265-017-0051-9. (AIS eLibrary)
35. Jain R, Paul S. Network virtualization and software-defined networking for cloud computing: A survey. IEEE Communications Magazine. 2013; 51(11):24-31. Doi: https://doi.org/10.1109/MCOM.2013.6658648. (WashU Research Profiles)
36. Johansson B, Waldau F, Åhlström O. What needs making information systems integration successful in the case of mergers and acquisitions. Procedia Computer Science. 2023; 219:619-625. Doi: https://doi.org/10.1016/j.procs.2023.01.331. (ScienceDirect)
37. Joseph N, Marnewick C. The continuum of Information Systems project success: Reflecting on the correlation between project success dimensions. South African Computer Journal. 2021; 33(1):37-58. Doi: https://doi.org/10.18489/sacj.v33i1.873. (SciELO)
38. Khajeh-Hosseini A, Greenwood D, Sommerville I. Cloud migration: A case study of migrating an enterprise IT system to IaaS. In 2010 IEEE 3rd International Conference on Cloud Computing, 2010, 450-457. Doi: https://doi.org/10.1109/CLOUD.2010.37. (University of St Andrews Research Portal)
39. Korhonen T, Jääskeläinen A, Laine T, Saukkonen N. How performance measurement can support achieving success in project-based operations. International Journal of Project Management. 2023; 41(1):102429. Doi: https://doi.org/10.1016/j.ijproman.2022.11.002. (ScienceDirect)
40. Kovela S, Skok W. Mergers and acquisitions in banking: A framework for effective IT integration. International Journal of Business and Management. 2015; 10(3):279-294. Doi: https://doi.org/10.5539/ijbm.v10n3p279. (CCSENet)
41. Lebese T, Motubatse KN. Effectiveness of information technology controls on financial performance management: Evidence from South African municipalities. Discover Global Society. 2025; 3, Article 143. Doi: https://doi.org/10.1007/s44282-025-00274-6. (Springer Link)
42. Lohrke FT, Frownfelter-Lohrke C, Ketchen DJ. The role of information technology systems in the performance of mergers and acquisitions. Business Horizons. 2016; 59(1):7-12. Doi: https://doi.org/10.1016/j.bushor.2015.09.006. (ScienceDirect)
43. Madduri H, Shi SSB, Baker R, Ayachitula N, Shwartz L, Surendra M, *et al*. A configuration management database architecture in support of IBM Service Management. IBM Systems Journal. 2007; 46(3):441-457. Doi: https://doi.org/10.1147/sj.463.0441. (IBM Research)
44. Mammah CU, Hassan E. Post-merger integration in Nigerian banking: Customer retention and operational continuity strategies. International Journal of Financial Management and Economics. 2022; 5(2):210-216. Doi: https://doi.org/10.33545/26179210.2022.v5.i2.628. (theeconomicsjournal.com)
45. Mandal S, Khan DA, Jain S. Cloud-based Zero Trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic. New Generation Computing. 2021; 39(3-4):599-622. Doi: https://doi.org/10.1007/s00354-021-00130-6
46. Mashiloane R, Jokonya O. Investigating the challenges of project governance processes of IT projects. Procedia Computer Science. 2018; 138:875-882. Doi: https://doi.org/10.1016/j.procs.2018.10.114. (ResearchGate)
47. Mbah Mbelli T, Dwolatzky B. Cyber Security, a Threat to Cyber Banking in South Africa: An approach to network and application security. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, 2016, 1-6. Doi: https://doi.org/10.1109/CSCloud.2016.18
48. Moonasar V, Naicker V. Cloud capability maturity model: A study of South African large enterprises. South African Journal of Information Management. 2020; 22(1):a1242. Doi: https://doi.org/10.4102/sajim.v22i1.1242. (SAJIM)
49. Mudzamba R, Van Der Schyff K, Renaud K. The challenges of cloud adoption among South African small to medium enterprises: A thematic analysis. The Electronic Journal of Information Systems in Developing Countries. 2022; 88(6):e12235. Doi: https://doi.org/10.1002/isd2.12235. (Wiley Online Library)
50. Olutimehin AO, Ganiu OS. Integrating Lean Six Sigma with reliability-centered maintenance: A unified framework for manufacturing excellence. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(6):983-996. Doi: https://doi.org/10.54660/.IJMRGE.2022.3.6.983-996
51. Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-factor authentication: A survey. Cryptography. 2018; 2(1):p.

1. Doi: https://doi.org/10.3390/cryptography2010001
52. Omoegun GO, Sunday EA, Essien MA, Oluokun OA. Vibration-based condition monitoring of rotating machinery using LabVIEW. International Journal of Scientific Research in Civil Engineering. 2023; 7(6):82-108. Doi: https://doi.org/10.32628/IJSRCE237529. (ResearchGate)
53. Omoegun GO, Sunday EA, Essien MA, Oluokun OA. Implementing smart automation solutions in medium-scale industries using SCADA systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024; 10(5):1207-1231. Doi: https://doi.org/10.32628/CSEIT241061242
54. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology, 2020. Doi: https://doi.org/10.6028/NIST.SP.800-207
55. Sanchez OP, Terlizzi MA, Moraes HROC. Cost and time project management success factors for information systems development projects. International Journal of Project Management. 2017; 35(8):1608-1626. Doi: https://doi.org/10.1016/j.ijproman.2017.09.007. (ScienceDirect)
56. Shittu H, Nabil M. Smart supply chain management with attribute-based encryption access control. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2023, 198-204. Doi: https://doi.org/10.1109/CCWC57344.2023.10099268
57. Shittu H, Opara IS, Elumilade RA, Liadi KO, Adeniji IO. Hydrogen as a secondary energy carrier: Modeling its integration in national grids. Iconic Research and Engineering Journals. 2019; 3(1):628-643. Doi: https://doi.org/10.64388/IREV3I1-1713909. (ResearchGate)
58. Shittu HA, Shittu MA. AI-powered digital twins for predictive maintenance and operational optimization of renewable energy systems. International Journal of Science, Architecture, Technology and Environment. 2024; 1(7):151-163. Doi: https://doi.org/10.63680/ijsate0324085.011
59. Shittu HA, Olagunju F, Shittu MA. Cyber physical resilience in digital substations: IoT-enabled adaptive protection for secure DER integration. International Journal of Science, Architecture, Technology and Environment. 2024; 1(3):81-99. Doi: https://doi.org/10.63680/ijsate032532.08
60. Shittu HA, Shittu MA, Adeleke OJ, Adedokun OJ. Blockchain-based energy trading models for peer-to-peer renewable microgrids. International Journal of Research in Electrical and Electronics Engineering. 2021; 4(3):1-19. Doi: https://doi.org/10.34218/IJREEE_04_03_001. (IAEME Publication)
61. Shittu MA, Adaramola TS, Shittu HA. Optimizing grid operation: Automation and management strategies for enhanced performance in modern energy systems. Iconic Research and Engineering Journals. 2025; 8(9):601-607. Doi: https://doi.org/10.5281/zenodo.15213105. (ResearchGate)
62. Shittu MA, Shittu HA, Adeleke OJ, Adedokun OJ. Digital twin modeling for real-time monitoring and fault detection in smart substations. International Journal of Industrial Engineering Research and Development. 2023; 14(2):25-44. Doi: https://doi.org/10.34218/IJIERD_14_02_003
63. Shittu MA, Shittu HA, Akintayo TA, Opara IS. IoT-enabled microgrid and BESS integration in ADMS: A framework for climate-resilient grid operation. In 2025 IEEE Symposium on Wireless Technology & Applications (ISWTA). IEEE, 2025, 1-9. Doi: https://doi.org/10.1109/ISWTA68114.2025.11330023
64. Sunday EA, Omoegun GO. Integrating solar power solutions in small-scale manufacturing industries in Nigeria. International Journal of Scientific Research in Science, Engineering and Technology. 2018; 4(8):832-853. Doi: https://doi.org/10.32628/IJSRSET23102175
65. Sunday EA, Omoegun GO. Optimizing electrical load distribution for hybrid solar installations in developing economies. International Journal of Scientific Research in Mechanical and Materials Engineering. 2019; 3(6):27-47. Doi: https://doi.org/10.32628/IJSRMME19349. (ResearchGate)
66. Sunday EA, Omoegun GO. Automation of process control systems using Siemens TIA Portal: A case study approach. International Journal of Scientific Research in Mechanical and Materials Engineering. 2022; 6(5):30-55. No article-specific DOI could be independently verified; one has therefore not been fabricated. (ResearchGate)
67. Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero Trust Architecture (ZTA): A comprehensive survey. IEEE Access. 2022; 10:57143-57179. Doi: https://doi.org/10.1109/ACCESS.2022.3174679
68. Tanriverdi H, Uysal VB. Cross-business information technology integration and acquirer value creation in corporate mergers and acquisitions. Information Systems Research. 2011; 22(4):703-720. Doi: https://doi.org/10.1287/isre.1090.0250. (PubsOnline)
69. Tanriverdi H, Uysal VB. When IT capabilities are not scale-free in merger and acquisition integrations: How do capital markets react to IT capability asymmetries between acquirer and target? European Journal of Information Systems. 2015; 24(2):145-158. Doi: https://doi.org/10.1057/ejis.2013.22. (Taylor & Francis Online)
70. Thomas G, Fernández W. Success in IT projects: A matter of definition? International Journal of Project Management. 2008; 26(7):733-742. Doi: https://doi.org/10.1016/j.ijproman.2008.06.003. (ScienceDirect)
71. Timcke S, Gaffley M, Rens A. The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. The African Journal of Information and Communication. 2023; 32. Doi: https://doi.org/10.23962/ajic.i32.16949. (SciELO)
72. Vu GTM, Hoang K, Hoang HV. Merger and

acquisition, firm-level cybersecurity risk, and research and development intensity. Managerial and Decision Economics. 2024; 45(5):3094-3106. Doi: https://doi.org/10.1002/mde.4190. (Wiley Online Library)
73. Wang V, Nnaji H, Jung J. Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice. 2020; 62:100415. Doi: https://doi.org/10.1016/j.ijlcj.2020.100415
74. Wijnhoven F, Spil T, Stegwee R, Fa RTA. Post-merger IT integration strategies: An IT alignment perspective. The Journal of Strategic Information Systems. 2006; 15(1):5-28. Doi: https://doi.org/10.1016/j.jsis.2005.07.002. (UT Research Information)
75. Wu M-S. The benefit and cost factors of CMDB implementations: An investigation of three organizations in Taiwan. Procedia - Social and Behavioral Sciences. 2014; 147:64-69. Doi: https://doi.org/10.1016/j.sbspro.2014.07.104. (ScienceDirect)
76. Yetton PW, Henningsson S, Böhm M, Leimeister JM, Krcmar H. How IT carve-out project complexity influences divestor performance in M&As. European Journal of Information Systems. 2023; 32(6):962-988. Doi: https://doi.org/10.1080/0960085X.2022.2085201. (Taylor & Francis Online)
77. Yusuf M, Akintunde A, Habeeb S, Quadri A. Radio Frequency Identification (RFID) based library management system. International Journal of Technology and Systems. 2023; 8(2):21-35. Doi: https://doi.org/10.47604/ijts.2041. (IPR Journals and Books)