Information Security and Data Protection Management in the Integration Phase of IT Mergers and Acquisitions

A Phased Model for the Systematic Management of Cybersecurity and Data Protection Risks in Post-Acquisition Contexts

Diploma in Safety and Security Management Program (TJK)

Final thesis report

Jussi Helminen

Eficode Oy

Helsinki, 13.3.2026

Aalto University Executive Education and Professional Development

Tiivistelmä

Yritysjärjestelyt IT-sektorilla aiheuttavat merkittäviä tietoturva- ja tietosuojahaasteita erityisesti kaupan jälkeisessä integraatiovaiheessa, jossa järjestelmiä, identiteettejä ja tietovirtoja yhdistetään. Tutkimukset osoittavat, että kyber- ja tietosuojariskit realisoituvat usein vasta kaupan toteutumisen jälkeen, kun perityt haavoittuvuudet, hajautettu valvonta, vanhat teknologiat ja epäselvät vastuut tulevat esiin. Tässä työssä integraatiovaiheen riskejä tarkastellaan kirjallisuuskatsauksen, sääntelyanalyysin sekä Marriott-Starwood- ja Yahoo-Verizon -tapaustutkimusten avulla. Tulokset osoittavat, että integraatioon liittyvät epäonnistumiset ovat rakenteellisia ja liittyvät identiteetinhallinnan puutteisiin, näkyvyyden heikkouteen, tekniseen velkaan, sääntelyriskeihin ja hallinnolliseen epäselvyyteen. Työssä esitetään vaiheittainen integraatiomalli, joka perustuu ISO 27001- ja ISO 31000 -standardeihin sekä GDPR- ja NIS2-vaatimuksiin. Malli tarjoaa rakenteellisen lähestymistavan tietoturvan ja tietosuojan hallintaan yritysjärjestelyiden integraatiovaiheessa.

Abstract

Mergers and acquisitions (M&A) in the IT sector create significant information security and data protection challenges, particularly during the post-acquisition integration phase when systems, identities, and data flows are consolidated. Evidence indicates that cyber and privacy risks often materialise after closing, when inherited vulnerabilities, fragmented monitoring, legacy technologies, and governance ambiguities become exposed. This thesis examines integration-phase risks through a structured literature review, regulatory analysis, and comparative case studies of the Marriott-Starwood and Yahoo-Verizon transactions. The findings demonstrate that integration failures are systemic and stem from identity misalignment, visibility gaps, inherited technical debt, regulatory exposure, and governance transition risks. Based on these insights, the thesis develops a phased integration model grounded in ISO 27001, ISO 31000, GDPR, and NIS2 principles. The model provides a structured framework for managing cybersecurity and privacy risks throughout post-acquisition integration and supports organisations in safeguarding transaction value.

Table of Contents

1 Introduction

1.1 Background: Mergers and Acquisitions in the IT

Mergers and acquisitions (M&A) have become a central instrument for organisational growth, particularly in the IT sector, where competitive advantage is closely tied to technological capability, digital infrastructure, and data assets. In many cases, acquisitions are driven by the need to obtain specialised expertise, proprietary platforms, customer ecosystems, or innovative service portfolios. As digitalisation accelerates across industries, information systems no longer function merely as support tools but constitute core components of enterprise value. Consequently, integrating two technologically complex organisations involves more than operational alignment; it requires careful management of information security and data protection risk.

While traditional M&A research has emphasised financial valuation, strategic fit, and cultural integration, cybersecurity has increasingly emerged as a material concern in transaction contexts. Documented incidents have shown that inherited vulnerabilities, fragmented monitoring systems, and legacy architectural dependencies can significantly affect post-acquisition stability and even transaction value. Importantly, the financial burden associated with identifying, remediating, and restructuring inherited systems may itself increase business risk, as unanticipated repair costs can delay integration, strain operational resources, and alter the anticipated economic benefits of the transaction. Empirical studies demonstrate that cybersecurity weaknesses can influence firm valuation and investor confidence (Campbell et al. 2003; Kamiya et al. 2018), while broader governance research highlights the structural role of cybersecurity risk in M&A outcomes (ECGI 2024). These findings suggest that cyber risk is not peripheral but embedded within the transformation process itself.

Within the European regulatory environment, these challenges are intensified by formal compliance obligations. The General Data Protection Regulation (GDPR) requires organisations to ensure lawful processing and adequate safeguards for personal data, even when organisational structures change (ICO 2021). The NIS2 Directive further strengthens expectations regarding cybersecurity governance, risk management, and leadership accountability (ENISA 2023). In certain transaction scenarios, the regulatory status of the acquiring organisation may change as a direct consequence of the acquisition. For example, an acquiring company that was previously outside the scope of NIS2 may become subject to its requirements by purchasing an entity classified as essential or important under the directive. In such cases, the transaction does not merely transfer technical assets, but fundamentally alters the organisation's regulatory risk profile, governance obligations, and potential liability exposure. Together, these frameworks mean that M&A integration is not only a technical undertaking but also a governance and compliance-sensitive process.

The M&A lifecycle typically proceeds through strategy development, target identification, due diligence, signing, closing, and a post-closing transition phase, which may involve either full organisational integration or structured carve-out and separation of business units. Although cybersecurity considerations increasingly form part of due diligence, practical experience and research indicate that the most significant risks often materialise after closing, when systems are actually combined (Deloitte 2024; WTW 2023). Due diligence provides a partial view of the target's security posture, but comprehensive technical validation is rarely possible before operational integration begins. As a result, inherited vulnerabilities frequently become visible only once environments are connected.

Integration therefore represents a decisive moment in the transaction lifecycle. It is during this period that identities are migrated, monitoring infrastructures are aligned, governance responsibilities are redefined, and data flows are restructured. The structural complexity of merging heterogeneous digital ecosystems creates temporary conditions in which exposure may increase. Understanding this dynamic forms the foundation of the present study.

1.1 Why focus on the Integration Phase

Although cybersecurity is now widely recognised as a component of M&A risk assessment, much of the existing discussion centres on due diligence. This emphasis, while understandable, risks overlooking the phase in which risk is most likely to become operationally relevant. Due diligence is inherently constrained by limited access to live systems, compressed timelines, and reliance on documentation provided by the target (Deloitte 2024). It can identify governance weaknesses and known incidents, but it rarely uncovers deeply embedded architectural flaws or undocumented dependencies.

By contrast, the integration phase introduces structural change. Systems that were previously independent are connected; authentication mechanisms are consolidated; and monitoring frameworks are reconfigured. These modifications alter the organisation's risk profile in real time. Research on technological integration shows that compatibility gaps and documentation deficiencies significantly increase the likelihood of operational disruption and security weakness (Zhao et al. 2023). In practice, integration often requires temporary configurations that may weaken control maturity before it is restored.

Organisational factors further amplify this vulnerability. During early post-acquisition stages, responsibility for inherited systems may not yet be clearly allocated. Differences in security culture, documentation standards, and risk appetite between the merging entities can delay harmonisation. Regulatory obligations under GDPR and NIS2 remain in force throughout this transition (ICO 2021; ENISA 2023), requiring organisations to maintain accountability even as structures evolve.

High-profile cases reinforce this pattern. The Marriott-Starwood breach demonstrates how inherited vulnerabilities can persist during integration when monitoring and governance alignment lag behind operational consolidation (In re Marriott International, Inc. 2021). The Yahoo-Verizon acquisition illustrates how previously undisclosed cybersecurity weaknesses can materially influence transaction outcomes (U.S. Securities and Exchange Commission 2018). Together, these cases suggest that integration deserves focused analytical attention.

1.2 Acquisition Types and Their Impact on Integration

The configuration of a transaction has a direct influence on the complexity of post-acquisition integration. In a full acquisition, the acquiring organisation assumes control over the entire legal entity, including its technological infrastructure, contractual obligations, data assets, and governance arrangements. This creates clarity in terms of authority and ownership; however, it also transfers full responsibility for legacy systems, embedded vulnerabilities, and accumulated technical debt. As a result, integration requires a systematic assessment of inherited architectures and alignment with the acquirer's security standards and operational practices, often within compressed timelines driven by strategic objectives.

Carve-out transactions, by contrast, introduce a different form of structural challenge. Rather than absorbing a complete organisation, the acquirer takes over a defined segment - such as a business unit or product division—while portions of the technological environment may remain shared with the seller. In such cases, systems including identity directories, databases, middleware components, and enterprise platforms may have been centrally managed across organisational boundaries prior to the transaction. Effective separation therefore demands detailed system mapping, identification of interdependencies, and carefully staged implementation to avoid operational interruption or residual access exposure.

Transitional Service Agreements (TSAs) are frequently used to maintain continuity during this period of disentanglement. While they can support stability, they may also introduce temporary ambiguity regarding accountability for cybersecurity controls, including monitoring, patch management, and incident handling. Research on IT integration in mergers and acquisitions suggests that high levels of system interconnection and poor documentation increase the difficulty of consolidation and heighten the probability of integration-related risk (Wijnhoven et al. 2006; Henningsson & Carlsson 2011). Where technical environments are tightly coupled and governance boundaries are not clearly defined, both full acquisitions and carve-outs can expose the acquiring organisation to elevated structural risk during the integration phase.

These structural differences highlight that integration risk is not uniform across transactions. Rather, it is shaped by the degree of architectural interconnection, the maturity of inherited systems, and the clarity of governance boundaries. Recognising these distinctions is essential for designing a structured approach to secure integration.

1.3 Illustrative Case Examples

The practical significance of cybersecurity risk in M&A transactions becomes particularly clear when examining documented cases in which inherited weaknesses materially affected post-acquisition outcomes. The Marriott-Starwood breach and the Yahoo-Verizon acquisition provide two distinct but complementary illustrations of how cyber risk can shape integration dynamics and transaction value.

In the Marriott-Starwood case, Marriott International acquired Starwood Hotels & Resorts Worldwide in 2016. At the time of closing, Starwood's reservation system had already been compromised by attackers for approximately two years. The breach remained undetected until 2018, ultimately affecting more than 380 million guest records (In re Marriott International, Inc. 2021). The persistence of the compromise into the post-acquisition period highlights the difficulty of achieving immediate visibility across inherited systems. Although the breach originated prior to the acquisition, the integration phase exposed weaknesses in monitoring alignment and governance consolidation.

The Yahoo-Verizon transaction presents a different manifestation of cyber risk. Following Verizon's agreement to acquire Yahoo's core internet business, previously undisclosed data breaches affecting billions of user accounts became public. These disclosures altered the perceived risk profile of the transaction and resulted in a renegotiated purchase price (U.S. Securities and Exchange Commission 2018). In this case, cybersecurity weaknesses influenced valuation and governance considerations directly, even before integration had fully progressed. Moreover, the consequences of such weaknesses can be contractually far-reaching: depending on disclosure practices and representations made during negotiation, liability may persist through indemnities, regulatory enforcement, or post-closing claims, meaning that cybersecurity risk does not necessarily dissipate with ownership transfer.

Although the timing and consequences differ, both cases reveal structural themes. Inherited vulnerabilities can persist beyond due diligence; visibility into legacy environments may be incomplete; and governance mechanisms may lag behind operational consolidation. These examples underscore that cybersecurity risk in M&A is neither hypothetical nor peripheral. It is embedded in the transformation process itself.

1.4 Research Problem and Objectives

The preceding discussion suggests a gap between awareness of cybersecurity risk in M&A and structured governance during post-acquisition integration. While due diligence frameworks have evolved to include cybersecurity assessments, fewer studies address how inherited systems should be harmonised securely once ownership transfers. Regulatory obligations remain in force throughout integration, and yet organisations often prioritise operational continuity over systematic risk stabilisation.

The research problem addressed in this thesis can therefore be framed as follows: although cybersecurity is widely recognised as a material factor in mergers and acquisitions, organisations lack a structured and standards-aligned approach specifically tailored to managing information security and data protection risks during post-acquisition integration.

The objective of this study is to develop a phased integration model that translates theoretical governance principles and regulatory requirements into a coherent operational framework. Drawing on ISO/IEC 27001 and ISO 31000, as well as GDPR and NIS2 obligations, the thesis seeks to bridge the gap between conceptual risk awareness and structured integration practice. The intention is not to propose a technical blueprint, but to articulate a governance-driven sequencing model that reduces exposure during organisational transformation.

1.5 Research Questions

To address the identified research problem, the thesis is guided by two central research questions.

The first question seeks to clarify the nature of integration-phase exposure:

What are the key information security and privacy risks that arise during the post-acquisition integration phase of IT-sector mergers and acquisitions?

This question focuses on identifying recurring patterns across academic literature, regulatory analysis, and documented case studies. The emphasis lies on structural drivers of risk rather than isolated technical incidents. Inherited vulnerabilities, identity misalignment, monitoring fragmentation, governance ambiguity, and regulatory exposure form the analytical lens through which integration risk is examined.

The second research question moves from diagnosis to design:

How can the integration process be structured into practical and sequential phases to ensure systematic management of information security and privacy risks?

Here, the objective is to construct a model that aligns governance standards, regulatory requirements, and empirical risk observations into a structured sequence of integration stages. The model is intended to provide a coherent framework adaptable to varying acquisition types and organisational contexts.

Together, these questions establish a progression from risk identification to structured mitigation.

1.6 Scope and Limitations

This thesis concentrates specifically on the post-acquisition integration phase within IT-sector mergers and acquisitions. Earlier stages of the M&A lifecycle, including strategic targeting and financial negotiation, are considered only insofar as they influence integration risk. The analysis focuses on information security and data protection governance, rather than on cultural integration, financial modelling, or strategic fit.

The study adopts a qualitative approach based on academic literature, regulatory frameworks, and comparative case analysis. Two documented cases-the Marriott-Starwood breach and the Yahoo-Verizon acquisition-provide empirical grounding. While this approach enables structured analytical generalisation, it does not allow for statistical generalisation across all M&A transactions.

The thesis does not incorporate primary interviews or proprietary organisational data. Instead, it relies exclusively on publicly accessible and verifiable sources. Although this limits access to confidential operational detail, it ensures transparency and replicability. The proposed integration model therefore operates at the governance and structural level, rather than prescribing specific technical implementation mechanisms.

Despite these limitations, the defined scope allows for focused examination of integration-phase cybersecurity and data protection risk. By situating the analysis within clearly articulated boundaries, the thesis aims to provide depth of insight while maintaining methodological coherence.

2 M&A and Integration Background

2.1 M&A Lifecycle overview

Mergers and acquisitions unfold through a sequence of stages that collectively shape organisational transformation. Although terminology varies slightly across disciplines, the lifecycle typically includes strategic planning, target identification, due diligence, negotiation and signing, closing, and post-acquisition integration. Each stage introduces distinct forms of uncertainty and risk. From a cybersecurity and data protection perspective, however, these risks do not distribute evenly across the lifecycle.

In the early strategic and target identification phases, cybersecurity considerations tend to remain high-level. Organisations may assess the digital maturity of potential targets or review publicly available breach histories, but detailed technical validation is rarely possible at this point. Cyber risk is recognised as relevant, yet it remains largely conceptual.

The due diligence phase represents a more structured attempt to assess risk. Increasingly, cyber due diligence includes review of security policies, incident records, compliance certifications, and governance documentation.

However, the depth of technical verification is often constrained by time, confidentiality limitations, and restricted access to production systems (Deloitte 2024). As a result, due diligence may identify governance weaknesses or known incidents, but it frequently fails to uncover deeply embedded architectural vulnerabilities or undocumented legacy dependencies. Empirical research suggests that cybersecurity weaknesses may remain hidden until integration activities expose them, particularly where pre-acquisition assessments rely heavily on historical audits, certifications, and documentation rather than comprehensive live-system validation (ECGI 2024).

Legal closing marks the formal transfer of ownership, but it does not resolve structural complexity. Rather, it initiates the most operationally sensitive phase of the lifecycle: integration. During this stage, previously separate technical environments are connected. Networks are bridged, identity repositories consolidated, monitoring infrastructures aligned, and data flows reconfigured. These changes alter the organisation's risk surface in fundamental ways. In complex IT-sector transactions, this transitional phase may extend over 18 to 24 months, during which interim architectures and temporary governance arrangements remain in place. The prolonged nature of this transition increases the likelihood that structural vulnerabilities persist before full stabilisation is achieved.

Research on information systems integration indicates that compatibility gaps, documentation deficiencies, and architectural heterogeneity significantly influence integration outcomes (Zhao et al. 2023). When merging organisations rely on divergent authentication standards, logging mechanisms, or system architectures, transitional misalignments are almost inevitable. In practice, integration often introduces temporary configurations designed to preserve operational continuity. While necessary, these transitional arrangements can reduce control maturity and increase exposure.

Regulatory obligations remain active throughout this process. Under GDPR, inherited personal data must continue to be processed lawfully and securely (ICO 2021). The NIS2 Directive further reinforces leadership accountability for cybersecurity governance (ENISA 2023). Compliance therefore cannot be deferred until after technical consolidation is complete; it must accompany integration in real time.

Taken together, the lifecycle perspective clarifies why integration deserves focused attention. Earlier phases identify potential exposure, but it is during integration that structural vulnerabilities either persist or are resolved. The act of merging systems transforms theoretical risk into operational reality. Understanding this progression provides the contextual foundation for analysing integration-phase cybersecurity and data protection challenges in greater depth.

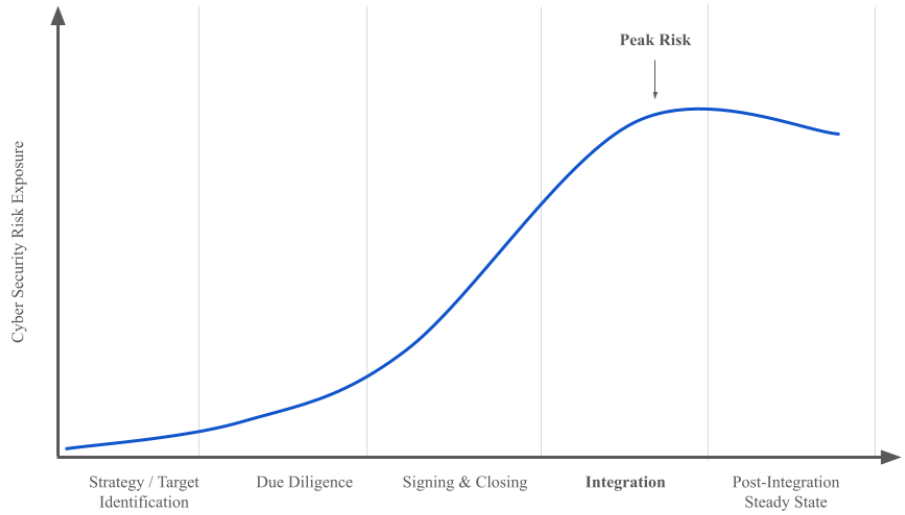

Figure 1. Cybersecurity Risk Escalation Across the M&A Lifecycle

2.2 Information Security and Privacy Requirements in M&A

Information security and data protection considerations extend across the entire M&A lifecycle, but their practical implications become most visible during integration. Once ownership transfers, the acquiring organisation assumes responsibility for inherited systems, data repositories, contractual relationships, and compliance obligations. This transfer is not merely administrative. It reshapes governance accountability, risk exposure, and regulatory liability.

From an information security standpoint, integration requires systematic evaluation of inherited technical environments. Targets may operate legacy applications, fragmented authentication mechanisms, or inconsistent patch management processes. These inherited characteristics do not disappear at closing; they become part of the acquirer's operational reality. ISO/IEC 27001 provides a structured governance foundation for addressing such risks by requiring asset identification, risk assessment, control implementation, and ongoing monitoring (Kobayashi et al. 2020). During integration, these principles support the harmonisation of access controls, logging practices, and incident response procedures across merged environments.

Risk management during integration is inherently dynamic. As systems are connected and data flows reconfigured, the organisation's exposure profile evolves. ISO 31000 emphasises continuous reassessment of risk in changing operational contexts (EY 2023). This perspective is particularly relevant

when temporary configurations or phased consolidations introduce transitional vulnerabilities. Effective integration governance therefore depends on iterative evaluation rather than one-time assessment.

Identity and access management (IAM) plays a central role in this process. Merging organisations frequently operate separate identity repositories and divergent privilege structures. During consolidation, temporary access rights may be granted to facilitate migration or stabilisation. Without clear governance, such exceptions can persist beyond their intended duration. Academic research highlights the importance of documentation quality and organisational alignment in mitigating integration-related vulnerabilities (Zhao et al. 2023). In practice, early harmonisation of IAM structures reduces the likelihood of privilege sprawl and inconsistent authentication standards.

Monitoring and detection capabilities are equally critical. Integration often requires alignment of logging pipelines and SIEM systems that were previously independent. Fragmented monitoring during transitional phases may create blind spots in detection coverage. Industry analyses repeatedly observe that threat actors exploit periods of organisational change when visibility is reduced (WTW 2023). The implication is clear: monitoring alignment must progress in parallel with system consolidation.

Data protection requirements introduce additional layers of complexity. GDPR mandates that personal data be processed lawfully, transparently, and securely, regardless of organisational change (ICO 2021). When integration involves database consolidation or system migration, organisations must reassess lawful bases for processing and ensure that data minimisation principles are upheld. Inherited data sets may include outdated or redundant information that no longer aligns with defined purposes. Structured data mapping and validation are therefore essential components of integration governance.

Where integration creates new processing contexts-such as unified customer analytics platforms or consolidated HR systems-Data Protection Impact Assessments (DPIAs) may be required. DPIAs provide a mechanism for anticipating and mitigating privacy risks before operational deployment. In this sense, data protection governance must accompany technical transformation rather than follow it.

NIS2 further reinforces cybersecurity governance expectations by requiring risk management measures, incident reporting capabilities, and leadership accountability (ENISA 2023). During integration, organisations must maintain compliance even while systems are in flux. The directive thus emphasises that cybersecurity governance cannot be deferred until after consolidation is complete.

Taken together, these security and privacy requirements demonstrate that integration is not solely a technical challenge. It is a governance-intensive process requiring coordination between security, legal, compliance, and operational functions. Technical harmonisation, regulatory compliance, and risk management must proceed simultaneously if inherited vulnerabilities are to be stabilised effectively.

2.3 Common Integration Challenges in IT Acquisitions

Integration challenges in IT-sector acquisitions tend to follow recurring patterns. Rather than arising from isolated technical errors, they typically reflect deeper structural characteristics of how digital environments evolve over time. Academic research, regulatory findings, and documented cases consistently show that merging heterogeneous systems introduces predictable vulnerabilities (Zhao et al. 2023; ECGI 2024).

One persistent challenge is architectural incompatibility. Organisations rarely operate uniform IT environments. Over time, they accumulate diverse operating systems, authentication protocols, database structures, cloud services, and custom-built applications. These environments may function adequately in isolation but become more complex when interconnected. Differences in encryption standards, privilege models, or logging formats can complicate harmonisation efforts. Research on information systems integration demonstrates that structural compatibility and documentation quality significantly influence the stability of post-merger consolidation (Zhao et al. 2023).

Importantly, architectural incompatibility is not confined to legacy or on-premises environments. Even organisations operating within modern, cloud-based infrastructures may exhibit substantial divergence beneath the surface. Differences in identity federation models, network segmentation strategies, API integrations, security configurations, and logging architectures can per-

sist even when systems are built on the same cloud platform. The use of contemporary technology therefore does not eliminate structural complexity; it merely alters its form.

Legacy infrastructure further complicates integration. Many organisations rely on systems that were designed for earlier technological contexts and have since accumulated technical debt. Such systems may lack modern authentication safeguards, encryption standards, or comprehensive monitoring capabilities. During integration, these components are often retained temporarily to preserve operational continuity. However, maintaining legacy systems without immediate hardening increases the likelihood that pre-existing weaknesses remain exploitable. The Marriott-Starwood case illustrates how inherited monitoring deficiencies can allow vulnerabilities to persist into the integration period (In re Marriott International, Inc. 2021).

Identity and access management (IAM) alignment represents a critical integration challenge in technology-intensive mergers. Acquiring and target organisations often maintain separate identity repositories, authentication mechanisms, and privilege models prior to consolidation. Bringing these structures together requires harmonising access policies, reconciling role definitions, and consolidating directory services without interrupting core business processes. During transitional phases, temporary access rights may be granted to facilitate migration activities or system stabilisation. If such permissions are not carefully governed and time-bound, they can inadvertently broaden the attack surface and create persistent exposure. Research on post-merger IT integration emphasises that misalignment between governance structures and technical architectures increases integration complexity and operational risk, particularly when coordination mechanisms are weak or documentation is incomplete (Wijnhoven et al. 2006; Baker & Niederman 2014). In this context, fragmented oversight of identity governance can become a structural vulnerability rather than a temporary inconvenience.

Monitoring and detection alignment also demand careful attention. Effective cybersecurity governance depends on centralised visibility. Yet during integration, logging infrastructures may remain partially segregated or inconsistently configured. Transitional network bridges and migration pathways may lack full instrumentation. Industry analyses have observed that threat actors

often exploit such periods of reduced visibility (WTW 2023). Without coordinated monitoring consolidation, detection capability may be weakened precisely when system interdependencies are increasing.

Governance integration compounds these technical challenges. Following acquisition, responsibilities for inherited systems must be clearly defined. Differences in organisational culture, documentation practices, and change management procedures can delay alignment. Where accountability for vulnerability remediation or incident response is ambiguous, risk mitigation may be inconsistent. Academic literature on integration risk highlights the importance of organisational coordination in achieving secure consolidation (Zhao et al. 2023).

Data protection requirements intersect with these technical and governance issues. Integration frequently involves merging databases, reconfiguring data flows, and consolidating customer or employee records. Inherited data repositories may be poorly documented or inconsistently classified. Under GDPR, organisations must reassess lawful bases and ensure that data minimisation principles are respected (ICO 2021). Failure to integrate privacy governance into technical consolidation can result in regulatory exposure.

Time pressure adds another layer of complexity. M&A transactions are often driven by expectations of rapid synergy realisation. Integration timelines may therefore prioritise operational continuity over structured risk mitigation. Temporary solutions introduced to facilitate consolidation can persist longer than intended. Over time, these provisional measures may become embedded within the merged environment, creating latent vulnerabilities (Grant Thornton 2021).

These recurring challenges reinforce the argument that integration risk is structural rather than accidental. The combination of architectural heterogeneity, legacy dependency, identity misalignment, monitoring fragmentation, governance transition, and regulatory pressure creates conditions in which vulnerabilities are likely to surface unless systematically addressed.

2.4 Special Challenges in Carve-Out Transactions

Carve-out transactions create integration dynamics that differ substantially from those encountered in full acquisitions. In a carve-out, only a defined

segment of the organisation - such as a division, product portfolio, or subsidiary - is transferred to the acquiring entity, while other parts of the enterprise remain under the seller's control. This partial transfer often means that technical infrastructure, data repositories, and governance processes have historically operated across organisational boundaries. As a result, separation must precede or occur in parallel with integration, increasing structural complexity.

Unlike full acquisitions, where ownership and system control are transferred in entirety, carve-outs frequently involve shared platforms and centrally managed services. Identity directories, enterprise systems, databases, and cloud-based environments may support both the divested unit and the retained business. Disentangling these shared assets requires systematic mapping of interdependencies and deliberate sequencing of separation activities to avoid operational disruption. The process is rarely straightforward, particularly where documentation is incomplete or where historical system ownership is ambiguous.

Transitional Service Agreements (TSAs) are commonly employed to ensure continuity during the separation period. While TSAs can provide short-term operational stability, they may also introduce temporary uncertainty regarding accountability for cybersecurity controls. Responsibilities related to access management, monitoring, patching, and incident response may be distributed between buyer and seller, increasing coordination demands and the potential for oversight gaps.

Research on post-merger IT integration highlights that tightly coupled system architectures and high degrees of technical interdependence significantly increase integration difficulty and risk exposure (Wijnhoven et al. 2006; Alaranta & Henningsson 2008). Where system components are deeply integrated and poorly documented, separation and consolidation become more resource-intensive and error-prone. In carve-out contexts, these structural conditions can elevate cybersecurity and data protection risks, particularly during transitional phases when governance boundaries are still being redefined.

Identity governance is particularly sensitive in carve-out contexts. Where authentication systems were previously centralised, separating user directories

and privilege structures demands rigorous control. Access rights must be reviewed, revoked where necessary, and reassigned under the acquiring organisation's governance model. Failure to properly complete this process may leave overlapping access permissions active across organisational boundaries, increasing exposure for both parties.

Data separation presents an additional layer of complexity. Shared databases may contain personal data relating to multiple business units or jurisdictions. Extracting only the relevant data for transfer requires accurate classification and validation processes. Under GDPR, organisations must ensure that transferred data is limited to what is necessary and processed under a lawful basis (ICO 2021). In practice, incomplete data mapping or inconsistent recordkeeping can create uncertainty regarding the scope of transferred information.

Transitional Service Agreements (TSAs) often accompany carve-out transactions. Under these agreements, the seller may continue to provide IT services or infrastructure support for a defined period after closing. While TSAs can facilitate operational continuity, they also create overlapping governance zones. Accountability for patch management, monitoring, and incident response may be distributed between buyer and seller. Where security standards differ, inconsistent control maturity may persist during the transitional phase. Industry analysis highlights governance ambiguity during TSA periods as a recurring integration risk factor (WTW 2023).

Vendor relationships further complicate carve-outs. Software licences, cloud service agreements, and managed security services may initially remain under the seller's contractual framework. The acquiring organisation must renegotiate or establish independent arrangements, often within constrained timelines. During this period, the carved-out entity may rely on infrastructure not yet fully aligned with its future governance baseline. NIS2 emphasises the importance of supply chain risk management and leadership accountability in such scenarios (ENISA 2023).

Operational pressure intensifies these challenges. Carve-outs are frequently driven by strategic or financial objectives that impose strict timelines. Business continuity must be preserved while separation and integration activities occur simultaneously. Temporary configurations introduced to enable this

transition-such as shared network connections or provisional access rights-may create unintended vulnerabilities if not governed carefully.

In contrast to full acquisitions, where risk largely arises from inherited technical debt, carve-outs require simultaneous separation and integration. This dual process increases structural complexity and amplifies the need for disciplined governance. The specific challenges associated with carve-outs reinforce the broader argument of this thesis: integration risk is shaped not only by technical vulnerabilities but also by structural and organisational design choices inherent in the transaction itself.

2.5 Why Integration Failures Are Common

Despite increasing awareness of cybersecurity and data protection risks in mergers and acquisitions, integration failures continue to occur with notable regularity. The persistence of these failures suggests that they are not simply the result of isolated technical misjudgements, but rather reflect recurring structural dynamics inherent in post-acquisition transformation. Academic research, regulatory observations, and documented case evidence collectively indicate that integration-related vulnerabilities arise from predictable interactions between technical complexity, organisational transition, and strategic pressure (ECGI 2024; Zhao et al. 2023).

One contributing factor is the inherent limitation of pre-acquisition due diligence. Although cyber due diligence practices have matured, they remain constrained by limited access to live environments, time pressure, and reliance on documentation supplied by the target (Deloitte 2024). Deep architectural analysis, comprehensive privilege audits, and full system validation are rarely feasible prior to closing. As a result, vulnerabilities embedded in legacy systems may only become visible once integration connects environments operationally. The Yahoo-Verizon case illustrates how historical cybersecurity weaknesses can materially influence transaction outcomes when disclosed during or after negotiation (U.S. Securities and Exchange Commission 2018). Similarly, the Marriott-Starwood breach demonstrates that inherited weaknesses may persist undetected into the integration phase (In re Marriott International, Inc. 2021).

Architectural heterogeneity further complicates integration. Organisations accumulate diverse technologies over time, often shaped by evolving business requirements, acquisitions, and outsourcing arrangements. When such environments are merged, inconsistencies in authentication protocols, encryption standards, or logging mechanisms may become apparent. Research indicates that integration risk increases when system compatibility is low and when documentation is incomplete (Zhao et al. 2023). Without deliberate sequencing and harmonisation, these mismatches can weaken control maturity during transitional stages.

Monitoring gaps represent another recurring source of vulnerability. Integration frequently involves phased consolidation of logging and detection infrastructures. Until monitoring systems are unified, visibility may be fragmented across environments. Transitional network connections or temporary configurations may lack comprehensive instrumentation. Industry analyses consistently note that threat actors exploit periods of organisational change when detection capabilities are in flux (WTW 2023). However, reduced visibility is not the only risk. Misaligned or partially integrated monitoring infrastructures may also generate excessive or poorly calibrated alert volumes, creating noise that obscures genuine malicious activity. In such cases, detection capability deteriorates not only because of blind spots, but because signal quality is degraded. The recurrence of these patterns suggests that monitoring alignment and calibration should be prioritised early in integration planning.

Governance ambiguity also contributes to integration failures. Following acquisition, responsibility for inherited systems must be clearly allocated. Differences in organisational culture, documentation practices, and reporting structures can delay alignment. If accountability for patch management, vulnerability remediation, or incident response is unclear, risk mitigation may be inconsistent or delayed. Academic research highlights organisational coordination as a determinant of integration success, particularly where security maturity differs between merging entities (Zhao et al. 2023). Importantly, governance in this context extends beyond formal management structures or documented control frameworks. It also concerns operational leadership and decision authority: who ultimately directs security priorities and assumes responsibility during transitional phases. In practical terms, parallel leadership structures - such as dual security heads operating without unified mandate - can create hesitation, duplicated effort, or strategic drift. Effective integration

therefore requires not only structural alignment but also clear organisational consolidation of authority.

Regulatory obligations intensify these challenges. GDPR requires that personal data processing remain lawful and secure throughout organisational change (ICO 2021). NIS2 reinforces leadership accountability and structured risk management requirements (ENISA 2023). During integration, organisations must maintain compliance even as technical and governance structures evolve. Failure to synchronise technical consolidation with regulatory oversight can result in enforcement exposure.

Strategic urgency adds another dimension. M&A transactions are frequently driven by expectations of rapid synergy realisation. Integration timelines may therefore prioritise operational consolidation over comprehensive risk assessment. Temporary measures introduced to expedite system alignment may remain in place longer than anticipated, embedding vulnerabilities within the merged environment (Grant Thornton 2021).

Taken together, these factors explain why integration failures recur across industries and transaction types. The convergence of technical heterogeneity, governance transition, monitoring realignment, regulatory complexity, and time pressure creates conditions in which vulnerabilities are likely to emerge unless integration is managed through structured and phased governance. This recognition reinforces the need for a systematic approach to integration risk mitigation.

2.6 Cybersecurity and Valuation in M&A

Beyond operational disruption and regulatory exposure, cybersecurity risk can also influence firm valuation in mergers and acquisitions. Empirical financial research has shown that publicly disclosed data breaches are often followed by statistically significant negative abnormal stock returns, suggesting that markets interpret cybersecurity failures as indicators of elevated risk and potential future costs (Campbell et al. 2003; Kamiya et al. 2018). These reactions reflect reassessments of expected cash flows, legal liabilities, and reputational damage. In this sense, cybersecurity posture becomes economically material information within acquisition contexts.

At the same time, the financial impact of cybersecurity appears to be asymmetric. While breaches and security failures tend to reduce firm value, there is limited evidence that strong cybersecurity capabilities generate equivalent valuation premiums (Gordon et al. 2011). This pattern suggests that cybersecurity functions primarily as a risk containment mechanism rather than a direct source of additional value. For acquiring organisations, cyber maturity may therefore serve less as a competitive differentiator and more as a safeguard against downside exposure.

In practice, cybersecurity considerations are often incorporated into transaction structuring rather than reflected directly in headline valuation multiples. Parties may address identified cyber risks through indemnification clauses, escrow arrangements, purchase price adjustments, or specific remediation commitments. These mechanisms acknowledge that inherited vulnerabilities represent contingent liabilities that may materialise after closing. The Yahoo-Verizon case illustrates this dynamic: previously undisclosed breaches led to renegotiation of the acquisition price and regulatory consequences, demonstrating how cybersecurity governance can influence transaction terms (U.S. Securities and Exchange Commission 2018).

These valuation dynamics complement the broader argument advanced in this thesis. While financial markets may respond to disclosed cybersecurity weaknesses, the more enduring exposure arises during post-acquisition integration, when inherited systems are operationally consolidated and governance responsibilities are redefined. In this context, cybersecurity risk is not confined to valuation effects but becomes embedded within organisational transformation itself. Structured integration governance, supported by phased risk management, is therefore essential not only for regulatory compliance but also for preserving transaction value and long-term organisational resilience.

3 Theoretical and Conceptual Framework

The analysis of cybersecurity and data protection risks in post-acquisition integration requires a structured conceptual foundation. Integration does not occur in a vacuum; it unfolds within established governance frameworks, regulatory obligations, and organisational risk management structures. To understand why cybersecurity risks intensify during M&A integration-and how they can be systematically mitigated-it is necessary to draw on established standards, regulatory instruments, and scholarly research on technological integration.

Cybersecurity exposure during integration emerges at the intersection of technical consolidation, governance transition, and regulatory accountability. As previously discussed, merging organisations must align identity systems, monitoring infrastructures, data processing activities, and oversight mechanisms. These processes are shaped by internationally recognised information security and risk management frameworks, most notably ISO/IEC 27001 and ISO 31000. Together, these standards provide principles for structured risk assessment, control alignment, accountability, and continuous improvement.

Regulatory requirements further define the boundaries within which integration must take place. The General Data Protection Regulation (GDPR) establishes obligations for lawful processing, transparency, and security of personal data (ICO 2021). The NIS2 Directive reinforces leadership accountability and mandates structured cybersecurity risk management for essential and important entities (ENISA 2023). These frameworks do not merely impose compliance requirements; they influence how organisations prioritise and sequence integration activities.

In parallel, academic research on technological M&A and information systems integration provides insight into structural vulnerability patterns. Studies highlight the importance of architectural compatibility, documentation quality, organisational alignment, and inherited technical debt in shaping integration outcomes (Zhao et al. 2023). Empirical financial research further demonstrates that cybersecurity weaknesses can materially affect acquisition outcomes and firm value (Campbell et al. 2003; Kamiya et al. 2018; ECGI 2024). These findings reinforce the view that cybersecurity risk in M&A is not episodic but structurally embedded.

This chapter brings these perspectives together to form a coherent analytical lens. ISO-based governance principles provide a control-oriented foundation; ISO 31000 contributes a dynamic risk management perspective; GDPR and NIS2 establish regulatory accountability; and academic research clarifies recurring integration risk drivers. Collectively, these frameworks support the identification of integration-phase vulnerabilities and provide the conceptual basis for the phased integration model developed later in this thesis.

3.1 The ISO/IEC 27001 Information Security Management System Framework

ISO/IEC 27001 is widely recognised as the leading international standard for information security management. Rather than prescribing isolated technical controls, it establishes a structured management system built around risk identification, control implementation, documentation, and continuous improvement. In the context of mergers and acquisitions, particularly during post-acquisition integration, ISO 27001 provides a governance-oriented foundation for aligning security practices across previously independent organisations.

At its core, the standard requires organisations to identify their information assets, assess associated risks, implement appropriate controls, and regularly review the effectiveness of those controls. This structured approach is especially relevant during integration, when inherited systems and data environments must be assessed under new governance conditions. Integration reshapes risk boundaries: systems are connected, identities are migrated, and monitoring frameworks are consolidated. Applying ISO 27001 principles in

this environment supports systematic evaluation rather than reactive remediation (Kobayashi et al. 2020).

A defining characteristic of ISO 27001 is its emphasis on risk-based thinking. Controls are not implemented in isolation but selected and prioritised based on identified risk exposure. During integration, the organisation's risk profile evolves rapidly. Legacy systems that once operated within contained environments may become interconnected with broader infrastructure, altering their threat exposure. The requirement for structured risk assessment therefore becomes critical in identifying which inherited components require immediate stabilisation and which can be addressed through phased consolidation.

Annex A of ISO 27001 further reinforces its applicability to integration contexts. The control domains include access management, cryptography, logging and monitoring, supplier governance, change management, and incident response. These areas correspond directly to the recurring vulnerabilities identified in the empirical case studies. Judicial findings in the Marriott data breach litigation indicate that monitoring and access control deficiencies contributed to prolonged compromise (In re Marriott International, Inc. 2021). Systematic application of Annex A controls during integration could mitigate such exposure by enforcing early harmonisation of authentication, logging, and oversight mechanisms.

Supplier governance under ISO 27001 is equally relevant. Acquiring organisations often inherit third-party relationships, including cloud service providers and managed security services. The standard requires formal assessment and ongoing monitoring of supplier risk. In integration scenarios, this means evaluating whether inherited contractual arrangements align with the acquiring organisation's security baseline and regulatory obligations.

Another important dimension of ISO 27001 is leadership involvement. The standard requires top management to demonstrate commitment to information security governance and allocate appropriate resources. This aligns closely with the accountability emphasis found in the NIS2 Directive (ENISA 2023). During M&A integration, visible leadership engagement helps ensure that security harmonisation is prioritised alongside operational consolidation.

It is important to recognise that ISO 27001 does not provide transaction-specific instructions. The standard outlines governance principles but does not prescribe how integration should be sequenced. For this reason, ISO 27001 serves in this thesis as a structural backbone rather than a procedural blueprint. Its value lies in offering a consistent control framework upon which a phased integration model can be constructed.

In summary, ISO/IEC 27001 contributes three key elements to the conceptual framework of this study: structured risk assessment, systematic control alignment, and governance accountability. These principles provide the foundation for understanding how integration-phase cybersecurity risks can be identified and mitigated within a disciplined management structure.

3.2 The ISO 31000 Risk Management Framework

ISO 31000 provides a broader perspective on organisational risk management that complements the information security focus of ISO/IEC 27001. While ISO 27001 concentrates specifically on information security governance, ISO 31000 offers principles applicable to enterprise-wide risk management. In the context of mergers and acquisitions, this broader lens is particularly valuable because integration affects not only technical systems but also strategic, operational, financial, and compliance dimensions of risk.

A defining feature of post-acquisition integration is that risk conditions evolve over time. Unlike steady-state operations, integration introduces phased structural changes: networks are interconnected, data repositories consolidated, governance roles redefined, and operational processes aligned. ISO 31000 emphasises that risk management should be iterative and responsive to changes in context. This principle is directly applicable to integration environments, where exposure may fluctuate as transitional configurations are introduced and subsequently stabilised (EY 2023).

The standard begins with establishing organisational context. In an M&A setting, context includes inherited technical architecture, existing compliance posture, leadership accountability, and stakeholder expectations. The acquiring organisation must understand not only the target's technical landscape but

also its historical governance practices and risk culture. Without this contextual awareness, risk assessment may overlook latent vulnerabilities embedded in legacy systems.

ISO 31000 distinguishes between risk identification, analysis, and evaluation. During integration, identification involves mapping inherited assets, recognising architectural dependencies, and understanding how system interconnections alter threat exposure. Analysis then considers the likelihood and potential impact of vulnerabilities under the new organisational configuration. For instance, an authentication mechanism that posed limited risk in a standalone environment may become significantly more exposed once connected to a broader enterprise network. Evaluation determines which risks require immediate intervention and which can be addressed through phased consolidation.

Continuous monitoring and review form another core component of ISO 31000. Integration is not a single event but a progression of technical and organisational adjustments. As systems are migrated and governance structures aligned, new risks may emerge. ISO 31000's cyclical approach supports ongoing reassessment rather than static evaluation. This dynamic perspective is particularly important in preventing transitional vulnerabilities from becoming embedded within the merged environment.

Communication and consultation constitute central elements of the ISO 31000 risk management framework. In the context of post-acquisition integration, risk governance extends beyond technical system alignment and requires coordinated action across IT, information security, legal, compliance, and executive leadership functions. The consolidation of technological environments frequently exposes differences in governance maturity, reporting structures, and decision-making practices. Research on post-merger IS integration indicates that integration difficulties often arise from misalignment between organisational units and unclear accountability structures rather than from technical incompatibility alone (Henningsson & Carlsson 2011; Baker & Niederman 2014). Effective communication mechanisms and clearly defined coordination processes are therefore essential to maintain responsibility clarity, align risk assessments, and ensure consistent application of security controls throughout the integration lifecycle.

Unlike ISO 27001, which focuses on specific security domains, ISO 31000 situates cybersecurity risk within the broader organisational risk landscape. In M&A transactions, cybersecurity interacts with financial valuation, regulatory liability, operational continuity, and reputational considerations. Empirical research indicates that cybersecurity incidents can influence acquisition pricing and market perception (ECGI 2024). By incorporating ISO 31000 principles, integration governance can account for these interconnected risk dimensions.

In this thesis, ISO 31000 provides the conceptual framework for treating integration as a dynamic risk environment. When combined with the control-oriented structure of ISO 27001, it enables the development of a phased model that aligns technical harmonisation with ongoing risk assessment and governance accountability.

3.3 GDPR and Data Protection Requirements in M&A Integration

The General Data Protection Regulation (GDPR) significantly shapes how mergers and acquisitions must be conducted within the European regulatory environment. Unlike voluntary governance standards, GDPR imposes binding obligations on organisations that process personal data. These obligations do not pause during organisational restructuring. On the contrary, integration often amplifies the complexity of compliance.

A central GDPR principle is lawful processing. When an organisation is acquired, responsibility for inherited personal data transfers to the acquiring entity. This requires reassessment of the legal basis under which that data was originally collected and processed. Integration frequently involves database consolidation, cross-system migration, or redefinition of processing purposes. Each of these actions may alter the legal context of data handling. As regulatory guidance emphasises, organisations must ensure that inherited data processing remains lawful and transparent under the new structure (ICO 2021).

Controller-processor relationships also require careful attention during integration. In transitional phases, particularly in carve-out transactions or where

Transitional Service Agreements (TSAs) are in place, responsibility for IT services may be shared between buyer and seller. GDPR requires clear allocation of accountability between controllers and processors. Ambiguity in these roles can lead to gaps in compliance and increased regulatory exposure.

Data minimisation introduces an additional challenge. Over time, organisations accumulate large volumes of personal data, some of which may no longer be strictly necessary for operational purposes. During integration, inherited data sets may be consolidated without full reassessment of relevance. GDPR requires that personal data be limited to what is necessary for defined purposes. Effective integration therefore depends on structured data mapping and validation processes to prevent excessive or redundant data transfer.

Data Protection Impact Assessments (DPIAs) may also become necessary during integration. Where processing activities are likely to result in high risk to data subjects-such as large-scale data consolidation or introduction of new analytics capabilities-DPIAs provide a formal mechanism for identifying and mitigating privacy risk. Conducting DPIAs as part of integration planning shifts compliance from reactive remediation to proactive governance.

Security of processing under Article 32 GDPR further reinforces the technical dimension of compliance. Organisations must implement appropriate safeguards, including access control, encryption, and resilience measures. If inherited systems lack adequate security maturity, the acquiring organisation must evaluate whether continued operation aligns with regulatory expectations. The Marriott-Starwood breach demonstrates how insufficient oversight of inherited data processing can result in regulatory consequences (Information Commissioner's Office 2020).

Documentation and accountability are equally important. Records of Processing Activities (RoPA) must be updated to reflect the merged organisational structure. Privacy notices may require revision to ensure continued transparency toward data subjects. If integration involves cross-border data transfers, appropriate safeguards must be verified.

In practice, GDPR compliance cannot be treated as a separate administrative task following technical consolidation. Integration decisions directly affect how personal data is processed and governed. Effective integration therefore requires simultaneous alignment of technical harmonisation and regulatory

oversight. GDPR, in this context, operates not only as a compliance requirement but as a structural constraint shaping integration governance.

3.4 NIS2 and Cyber Governance Requirements

The NIS2 Directive strengthens the regulatory framework governing cybersecurity risk management within the European Union. Expanding upon the original NIS Directive, it broadens the scope of covered entities and places greater emphasis on governance accountability and structured risk management. For IT-sector organisations, many of which fall within the directive's scope, NIS2 significantly influences how cybersecurity must be managed during organisational change, including mergers and acquisitions.

A central feature of NIS2 is its emphasis on leadership responsibility. Senior management is required to approve and oversee cybersecurity risk management measures, and in certain cases may face direct accountability for failures (ENISA 2023). During post-acquisition integration, this requirement becomes particularly salient. Once ownership transfers, the acquiring organisation assumes responsibility for inherited systems and associated risks. Leadership cannot rely solely on the historical security posture of the target; it must ensure that inherited environments meet current governance standards.

In practical terms, the NIS2 Directive requires covered entities to implement and maintain a structured cybersecurity risk management framework. Key requirements include:

- **Risk management measures**: Organisations must implement appropriate and proportionate technical and organisational measures to manage cybersecurity risks, including policies for risk analysis, incident handling, and system security.
- **Incident detection and reporting obligations**: Significant cybersecurity incidents must be reported to competent authorities within defined timeframes, requiring continuous monitoring and established escalation procedures.
- **Business continuity and resilience measures**: Entities must ensure operational continuity through backup management, disaster recovery capabilities, and crisis management planning.

- **Supply chain and third-party risk management**: Organisations are required to assess and manage cybersecurity risks arising from suppliers and service providers, including contractual and oversight mechanisms.
- **Access control and authentication safeguards**: Measures must address identity and access management, including appropriate authentication, privilege restriction, and secure system configuration.
- **Vulnerability management and patch governance**: Entities must implement processes for identifying, prioritising, and remediating vulnerabilities in a timely manner.
- **Management accountability and oversight**: Senior leadership must approve cybersecurity risk management measures and may bear direct responsibility for systemic failures.

These requirements collectively position cybersecurity as a governance-level obligation rather than a purely technical function, reinforcing its strategic significance during organisational transformation.

NIS2 requires organisations to implement risk management measures covering incident handling, business continuity, supply chain security, access control, vulnerability management, and cryptographic safeguards. These domains correspond closely to the structural vulnerabilities identified in earlier chapters. Integration frequently involves consolidation of monitoring systems, alignment of incident response processes, and reassessment of inherited third-party providers. Where inherited systems lack adequate controls, remediation cannot be postponed without increasing regulatory exposure.

Incident reporting obligations under NIS2 further reinforce the importance of maintaining detection capability during integration. Covered entities must report significant incidents within defined timeframes. Transitional phases, in which monitoring systems may not yet be fully unified, present elevated risk of delayed detection. Integration planning must therefore ensure that reporting mechanisms remain operational throughout structural change.

Supply chain risk is another area emphasised by NIS2. Acquisitions often involve inherited vendor relationships, including cloud providers, managed service providers, and outsourced security operations. The directive requires organisations to assess and manage supply chain exposure explicitly. During

integration, this means reviewing inherited contracts and verifying alignment with the acquiring organisation's security standards.

Business continuity considerations also intersect with integration governance. Consolidating systems can introduce temporary instability. NIS2 requires organisations to maintain resilience and recovery capabilities even during organisational transformation. Integration sequencing must therefore balance consolidation objectives with continuity safeguards.

The governance expectations embedded in NIS2 complement the principles of ISO 27001 and ISO 31000. While ISO standards provide structured management frameworks, NIS2 imposes mandatory accountability. Together, they reinforce the view that cybersecurity during integration is not solely a technical matter but a leadership responsibility requiring structured oversight.

In this thesis, NIS2 contributes a regulatory governance lens to the conceptual framework. It underscores that integration risk management must satisfy not only internal control objectives but also externally imposed accountability requirements. This regulatory dimension strengthens the case for a phased integration model grounded in explicit governance alignment.

3.5 Cybersecurity Risk Considerations in M&A Integration

Cybersecurity risk during M&A integration cannot be understood through a single lens. It emerges from the interaction of inherited technical environments, evolving governance structures, regulatory obligations, and strategic pressures. The standards and regulatory frameworks discussed above provide governance principles, but the practical manifestation of risk becomes visible only when systems are consolidated and operational boundaries shift.

A defining characteristic of post-acquisition integration is that the organisation's risk profile is temporarily unstable. Unlike routine operations, integration involves deliberate architectural modification. Systems that were previously independent become interdependent; access controls are reconfigured; data repositories are merged; and monitoring infrastructures are aligned. Each

of these changes alters exposure in real time. ISO 31000's emphasis on continuous reassessment is therefore particularly relevant in this context, as risk conditions evolve alongside technical consolidation (EY 2023).

Inherited vulnerabilities remain a central concern. Targets may operate legacy systems that meet minimal operational requirements but fall short of the acquiring organisation's security baseline. These systems may lack robust monitoring, modern authentication safeguards, or consistent patch management. Once connected to a broader enterprise environment, such weaknesses can increase exposure. The Marriott-Starwood breach illustrates how insufficient oversight of inherited systems can allow compromise to persist during integration (In re Marriott International, Inc. 2021).

Identity and access management misalignment frequently amplifies this exposure. Parallel identity repositories and divergent privilege models may coexist during transitional phases. Temporary access rights granted for migration purposes can unintentionally expand attack surfaces. Academic research consistently highlights documentation quality and governance maturity as determinants of integration stability (Zhao et al. 2023). Early harmonisation of identity governance therefore reduces structural vulnerability.

Monitoring alignment is equally critical. Integration often requires staged consolidation of logging infrastructures and SIEM systems. Until monitoring is unified, detection capability may be uneven. Transitional configurations-such as network bridges or data migration pathways-may not be fully instrumented. Industry analyses have observed that attackers frequently exploit periods of organisational change when visibility is reduced (WTW 2023). Maintaining detection continuity throughout integration is therefore essential.

Regulatory compliance further shapes integration risk. GDPR requires that personal data processing remain lawful and secure even as systems are restructured (ICO 2021). NIS2 imposes structured risk management and reporting obligations that persist throughout organisational change (ENISA 2023). Integration activities must therefore be aligned not only with technical consolidation but also with compliance oversight.

Strategic considerations add another layer. M&A transactions are often motivated by synergy realisation and competitive positioning. Integration timelines may prioritise operational efficiency, creating tension between speed

and control maturity. Temporary configurations introduced to expedite consolidation may persist beyond their intended duration, embedding vulnerabilities within the merged environment.

Taken together, these interacting factors demonstrate that integration-phase cybersecurity risk is structural, dynamic, and multi-dimensional. It arises not from isolated technical oversights but from the combined effects of architectural heterogeneity, governance transition, regulatory constraint, and strategic pressure. Recognising these patterns provides the analytical bridge between theoretical frameworks and the phased integration model developed in the next chapter.

3.6 Summary

The theoretical and conceptual foundations discussed in this chapter provide a structured lens for understanding cybersecurity and data protection risk during post-acquisition integration. Rather than treating integration risk as an isolated technical concern, the preceding sections situate it within established governance standards, regulatory obligations, and academic research on technological transformation.

ISO/IEC 27001 offers a control-oriented framework for aligning security governance across merged environments. ISO 31000 complements this perspective by emphasising continuous risk assessment in changing operational contexts. Together, these standards support disciplined oversight during transitional phases. GDPR and the NIS2 Directive introduce binding accountability requirements that shape how integration must be sequenced and governed. Compliance cannot be deferred; it must accompany technical consolidation.

Academic research on information systems integration further clarifies why integration frequently exposes structural vulnerabilities. Architectural heterogeneity, documentation gaps, governance misalignment, and inherited technical debt are recurring themes across both scholarly studies and documented case evidence (Zhao et al. 2023; ECGI 2024). The comparative cases examined earlier reinforce that these risk drivers manifest in practice, influencing both operational stability and financial outcomes.

Viewed collectively, these frameworks and empirical insights establish a coherent foundation for analysing integration-phase risk. They clarify why vulnerabilities intensify during transitional periods and why structured, phased governance is necessary. The next chapter outlines the research methodology through which these theoretical perspectives and empirical observations are synthesised into a practical integration model.

4 Research Methodology

4.1 Research Approach

This thesis adopts a qualitative research approach to examine how information security and data protection risks emerge during the post-acquisition integration phase of mergers and acquisitions in the IT sector. The phenomenon under study involves organisational transformation, evolving technical architectures, regulatory constraints, and governance transitions. Because these dynamics cannot be meaningfully reduced to quantitative indicators alone, a qualitative design is appropriate for capturing structural risk patterns and contextual complexity.

The research design combines a structured literature review with comparative case analysis. Rather than relying on primary interview data, the study synthesises established academic research, regulatory frameworks, and publicly documented cases. This approach allows the analysis to focus on recurring integration risk drivers and governance mechanisms without depending on confidential organisational information.

The literature review provides the conceptual foundation for the study. Academic publications addressing technological integration, architectural compatibility, cybersecurity risk, and organisational governance form the theoretical basis of the analysis (Zhao et al. 2023; ECGI 2024). These sources are complemented by recognised standards and regulatory instruments, including ISO/IEC 27001, ISO 31000, GDPR, and NIS2 (Kobayashi et al. 2020; ICO 2021; ENISA 2023). Together, they establish the governance and compliance context within which integration must occur.

The empirical dimension consists of two comparative case studies: the Marriott-Starwood breach and the Yahoo-Verizon acquisition. Both cases are extensively documented and publicly verifiable, providing sufficient transparency for structured analysis. They represent different manifestations of cybersecurity risk in M&A contexts: one highlighting integration-phase exposure and the other demonstrating valuation and disclosure implications. Analysing these cases alongside theoretical frameworks enables identification of recurring structural patterns.

The overall objective of this methodological approach is not to test statistical hypotheses, but to synthesise conceptual insights and empirical evidence into a structured integration model. By drawing on diverse yet complementary sources, the research aims to produce analytically grounded and practically relevant conclusions.

4.2 Research Design and Data Sources

The research design is structured as a qualitative, comparative case-based study grounded in systematic literature analysis. The intention is to integrate theoretical perspectives, regulatory requirements, and documented case evidence in order to identify recurring cybersecurity and data protection risk patterns during post-acquisition integration.

The study draws on three principal categories of sources. First, peer-reviewed academic publications provide conceptual insight into technological integration risk, organisational alignment, and cybersecurity governance in M&A contexts. Research examining architectural compatibility, inherited technical debt, and integration complexity forms a central analytical layer (Zhao et al. 2023). In addition, empirical financial research contributes understanding of how cybersecurity incidents influence firm valuation and transaction dynamics (ECGI 2024; Campbell et al. 2003; Kamiya et al. 2018).

Second, regulatory and standards-based materials establish the compliance and governance boundaries relevant to integration. GDPR guidance from the Information Commissioner's Office (ICO 2021) clarifies data protection obligations during organisational change, while the NIS2 Directive articulates cybersecurity governance and reporting expectations (ENISA 2023).

ISO/IEC 27001 and ISO 31000 provide structured risk management and control alignment principles that inform the development of the integration model (Kobayashi et al. 2020).

It is important to note that the regulatory orientation of this study is primarily European. The governance and compliance analysis is grounded in GDPR and NIS2 requirements, which apply within the European Union and may differ from cybersecurity and disclosure obligations in other jurisdictions, such as the United States. Although the case studies include transactions with transatlantic dimensions, the integration model developed in this thesis reflects EU regulatory expectations and should therefore be interpreted within that normative context. Differences in legal frameworks, supervisory practices, and enforcement regimes may affect how integration risk manifests in non-EU environments.

Third, selected industry analyses are used to contextualise academic findings within contemporary organisational practice. Reports from Deloitte (2024), Grant Thornton (2021), and Willis Towers Watson (WTW 2023) are incorporated where they offer structured analytical discussion rather than promotional content. These sources help bridge theoretical insights and practical integration challenges.

The empirical component of the study consists of two documented case studies: the Marriott-Starwood breach and the Yahoo-Verizon acquisition. Both cases are supported by publicly accessible regulatory disclosures and independent reporting (In re Marriott International, Inc. 2021; U.S. Securities and Exchange Commission 2018; Reuters 2017). The use of multiple independent sources for each case reduces reliance on a single narrative and strengthens analytical reliability.

All data used in this research is publicly available and independently verifiable. This ensures transparency and allows the analytical process to be replicated. By combining academic research, regulatory guidance, industry analysis, and comparative case evidence, the research design establishes a structured foundation for synthesising integration-phase risk patterns.

4.3 Data Collection Methods

Data collection in this thesis is based entirely on secondary sources drawn from academic literature, regulatory documentation, and publicly documented case materials. The qualitative design emphasises structured synthesis rather than primary field data. This approach allows the analysis to focus on recurring structural patterns in integration-phase cybersecurity risk while maintaining transparency and verifiability.

Academic sources were selected on the basis of relevance to mergers and acquisitions, information systems integration, cybersecurity governance, and organisational risk management. Particular attention was given to peer-reviewed research examining architectural compatibility, legacy system dependencies, identity governance challenges, and financial consequences of cybersecurity incidents (Zhao et al. 2023; ECGI 2024; Campbell et al. 2003; Kamiya et al. 2018). These publications provide both conceptual and empirical grounding for understanding how integration risk manifests.

Regulatory and standards-based materials were chosen to define the normative framework within which integration must occur. GDPR guidance from the Information Commissioner's Office (ICO 2021) clarifies legal obligations associated with inherited personal data. The NIS2 Directive outlines cybersecurity governance expectations applicable to IT-sector entities (ENISA 2023). ISO/IEC 27001 and ISO 31000 were incorporated through academic analysis and governance literature to frame risk assessment and control alignment (Kobayashi et al. 2020). These sources ensure that the study remains anchored in recognised governance principles rather than informal practice.

Industry analyses were included selectively where they provide structured insight into cybersecurity risk during M&A. Reports from Deloitte (2024), Grant Thornton (2021), and WTW (2023) were used to contextualise theoretical findings within contemporary integration practice. Care was taken to rely only on analytical material rather than marketing-oriented content.

The empirical component of data collection consists of documentation relating to the Marriott-Starwood and Yahoo-Verizon cases. For the Marriott–Starwood case relies on regulatory findings and judicial documentation (In re Marriott International, Inc. 2021; Bradley 2022). For the Yahoo-Verizon

transaction, publicly available regulatory disclosures and corporate communications were used (U.S. Securities and Exchange Commission 2018; Reuters 2017). Using multiple sources for each case supports cross-verification and reduces reliance on single-source interpretation.

By relying exclusively on accessible and documented materials, the data collection strategy supports transparency and replicability. The emphasis on peer-reviewed research and official regulatory sources strengthens the credibility of the analysis while avoiding dependence on proprietary or unverifiable information.

4.4 Data Analysis

The analysis in this thesis follows a structured qualitative synthesis approach. Rather than applying statistical techniques, the study identifies recurring themes and structural risk patterns across academic literature, regulatory frameworks, and comparative case evidence. The objective is to move from descriptive observation toward conceptual integration.

The first stage of analysis involved examining academic research to identify common determinants of integration risk. Studies on technological M&A and information systems integration highlight architectural incompatibility, legacy system dependencies, documentation deficiencies, and governance misalignment as recurrent drivers of post-merger instability (Zhao et al. 2023). Empirical financial research further demonstrates that cybersecurity weaknesses can influence market valuation and investor perception (Campbell et al. 2003; Kamiya et al. 2018; ECGI 2024). These strands of literature collectively provide a conceptual taxonomy of integration-related vulnerabilities.

The second stage incorporated regulatory and standards-based analysis. GDPR and NIS2 were examined to clarify compliance and governance obligations during organisational transformation (ICO 2021; ENISA 2023). ISO/IEC 27001 and ISO 31000 provided structured principles for risk assessment, control alignment, and continuous monitoring (Kobayashi et al. 2020). This stage ensured that the identification of risk patterns remained anchored in recognised governance frameworks rather than anecdotal evidence.

The third stage consisted of comparative case analysis. The Marriott-Starwood and Yahoo-Verizon cases were examined using the thematic categories derived from the literature. Each case was assessed in terms of inherited vulnerabilities, identity governance challenges, monitoring alignment, regulatory exposure, and transaction consequences. Applying a consistent analytical lens allowed similarities and differences to emerge without overemphasising case-specific details (In re Marriott International, Inc. 2021; U.S. Securities and Exchange Commission 2018).

Cross-case comparison strengthened analytical generalisation. While the two cases differ in timing and manifestation-one illustrating integration-phase exposure and the other valuation and disclosure impact-both reveal structural characteristics consistent with academic findings. The recurrence of similar governance and architectural challenges across contexts reinforces the argument that integration risk is systemic.

The final stage of analysis synthesised these insights into a phased integration model. The model was constructed by mapping identified risk drivers to governance principles derived from ISO standards and regulatory requirements. Each phase corresponds to a distinct stage in risk stabilisation and control harmonisation, reflecting the dynamic nature of integration.

Through this multi-stage analytical process, the study progresses from identifying integration-phase risks to developing a structured mitigation framework. This progression ensures coherence between theoretical foundations, empirical observations, and the practical contribution presented in the subsequent chapter.

4.5 Reliability, Validity, and Limitations

Ensuring reliability and validity is particularly important in qualitative research that relies on secondary sources and comparative case analysis. This thesis addresses these concerns through careful source selection, structured synthesis, and transparent analytical reasoning.

Reliability is supported by the use of publicly accessible and verifiable materials. All academic publications, regulatory documents, and case sources cited are traceable to identifiable authors or institutions. This transparency allows the analytical process to be reviewed and, in principle, replicated by other researchers. The reliance on recognised governance standards such as ISO/IEC 27001 and ISO 31000 further strengthens conceptual consistency (Kobayashi et al. 2020).

Validity is enhanced through triangulation across multiple categories of evidence. The analysis integrates peer-reviewed academic research (Zhao et al. 2023; ECGI 2024), regulatory frameworks (ICO 2021; ENISA 2023), and documented case material derived from judicial and regulatory proceedings (In re Marriott International, Inc., 2021; U.S. Securities and Exchange Commission 2018). Converging patterns across these independent sources increase confidence that the identified integration risks are structural rather than incidental.

The use of two comparative case studies contributes to analytical robustness. Examining both the Marriott-Starwood breach and the Yahoo-Verizon acquisition reduces the risk of overgeneralising from a single event. Although the cases differ in context and outcome, recurring themes such as inherited vulnerabilities, governance misalignment, and regulatory exposure appear in both. This supports analytical generalisation without claiming statistical representativeness.

Certain limitations must nevertheless be acknowledged. The research relies exclusively on secondary data and does not incorporate primary interviews or proprietary organisational information. While this ensures transparency, it limits insight into internal decision-making processes that may not be publicly documented. Additionally, the analysis does not include technical forensic examination of systems; instead, it focuses on structural and governance dimensions of integration risk.

Although the study draws on two documented cases, its conclusions are based on analytical synthesis rather than quantitative generalisation. The objective is to identify recurring structural patterns that can inform governance design, not to estimate the frequency of integration failures across all transactions.

Despite these limitations, the chosen methodology is appropriate for the research objectives. By combining recognised theoretical frameworks, regulatory guidance, and comparative empirical evidence, the thesis provides a coherent and analytically grounded basis for developing a phased integration model.

4.6 Ethical Considerations

The research presented in this thesis adheres to standard principles of academic integrity and responsible scholarship. As the study relies exclusively on publicly accessible secondary sources, it does not involve the collection of personal data, confidential corporate information, or sensitive unpublished materials. The absence of primary interviews or proprietary datasets eliminates concerns related to participant consent, anonymity, or data protection in the research process itself.

All sources used in the thesis are clearly cited and attributable to identifiable authors or institutions. Academic publications, regulatory documents, and case materials are referenced consistently to ensure traceability. Where industry analyses are incorporated, they are selected for analytical relevance rather than promotional intent and are interpreted in light of broader academic and regulatory evidence.

The case studies analysed-Marriott-Starwood and Yahoo-Verizon-are based entirely on publicly documented incidents. The analysis focuses on structural and governance dimensions rather than on assigning responsibility to individuals. This approach aligns with ethical research practice by emphasising systemic risk patterns rather than personal attribution.

Care has also been taken not to speculate beyond documented evidence. Interpretations are grounded in referenced materials and linked to established theoretical frameworks. No technical exploit details are disclosed beyond what is already publicly available. The objective is to extract governance lessons rather than expose operational vulnerabilities.

Overall, the methodological design presents minimal ethical risk. By relying on transparent and verifiable sources, and by maintaining analytical restraint in interpretation, the thesis meets standard academic expectations regarding responsible research conduct.

5 Case Studies of Cybersecurity Risk in M&A Integration

5.1 Introduction

The theoretical discussion in the preceding chapters establishes that cybersecurity risk during mergers and acquisitions is structurally embedded in integration processes. To ground these observations in documented practice, this chapter examines two well-known cases in which cybersecurity played a material role in M&A outcomes: the Marriott-Starwood breach and the Yahoo-Verizon acquisition. Together, these cases provide empirical context for the structural risk patterns identified earlier.

The purpose of including comparative case studies is not to recount breach narratives in detail, but to examine how inherited vulnerabilities, governance alignment challenges, and disclosure dynamics manifest during real transactions. By analysing cases that differ in timing and impact-one centred on post-acquisition operational exposure and the other on valuation and disclosure consequences-the study can identify recurring themes without relying on a single illustrative event.

Both cases are extensively documented through regulatory disclosures and independent reporting, enabling transparent analysis. They also represent distinct dimensions of cybersecurity risk in M&A: operational compromise during integration and financial renegotiation driven by historical breach disclosure. Examining them together allows for a more nuanced understanding of how cyber risk influences both integration governance and transaction stability.

The analysis that follows applies a consistent conceptual lens derived from Chapter 3. Each case is considered in terms of inherited vulnerabilities, identity and access management alignment, monitoring capability, governance accountability, and regulatory exposure. This structured approach facilitates

comparison and prepares the foundation for the synthesis presented in Chapter 6.

5.2 Marriott-Starwood: Inherited Vulnerability and Integration-Phase Exposure

5.2.1 Background of the Acquisition

Marriott International completed its acquisition of Starwood Hotels & Resorts Worldwide in 2016, forming one of the largest global hospitality groups. The transaction involved the consolidation of extensive reservation systems, customer databases, and operational infrastructures. At the time of acquisition, Starwood's IT environment had evolved over decades and included legacy components, heterogeneous system architectures, and historically accumulated technical dependencies.

Unbeknownst to Marriott during the acquisition process, Starwood's reservation database had been compromised by attackers as early as 2014. The intrusion remained undetected until 2018, two years after closing, ultimately affecting more than 380 million guest records (Marriott International Inc. 2018). The scale and duration of the breach highlight the difficulty of achieving immediate visibility into inherited environments during integration.

5.2.2 Integration Context and Structural Weaknesses

The persistence of the breach into the post-acquisition period reflects several structural risk factors associated with integration. First, the inherited monitoring infrastructure was not fully aligned with Marriott's security operations. Logging mechanisms and detection processes remained partially segregated, limiting comprehensive visibility across the merged environment. As systems were gradually integrated, the absence of unified oversight allowed the compromise to continue.

Second, identity and access management structures required harmonisation. Legacy authentication mechanisms and privilege allocations within the Starwood environment were not immediately aligned with Marriott's security baseline. During transitional phases, such inconsistencies can create opportunities for persistent access.

Third, governance consolidation did not occur instantaneously. Although ownership transferred at closing, operational responsibility for inherited systems required phased alignment. During this transitional period, accountability for monitoring, patch management, and incident response may not have been fully centralised. This governance lag illustrates how structural transition can amplify inherited vulnerabilities.

5.2.3 Regulatory and Organisational Consequences

The discovery of the breach led to significant regulatory scrutiny and financial consequences. In October 2020, the UK Information Commissioner's Office imposed a £18.4 million fine on Marriott International, concluding that the company had failed to implement appropriate technical and organisational measures to protect personal data following the acquisition (Information Commissioner's Office 2020). The decision emphasised that acquiring organisations bear responsibility for inherited systems once control is established, regardless of whether vulnerabilities originated prior to the transaction. The case thus demonstrates that inherited cybersecurity weaknesses become the acquirer's liability during integration.

Beyond regulatory enforcement, the breach also had reputational and operational implications. It highlighted the difficulty of consolidating complex legacy systems under time pressure and exposed the risks associated with delayed monitoring alignment. Rather than representing an isolated failure, the incident illustrates recurring structural challenges that arise during integration-phase transformation, particularly where inherited vulnerabilities are not stabilised early.

5.3 Yahoo-Verizon: Cyber Risk Affecting Transaction Valuation

5.3.1 Background of the Acquisition

In 2016, Verizon Communications announced its agreement to acquire Yahoo's core internet business as part of its strategy to strengthen its digital media operations. Shortly after the transaction was announced, previously un-

disclosed data breaches affecting billions of Yahoo user accounts were revealed. These breaches had occurred in 2013 and 2014 but had not been fully disclosed during earlier stages of the acquisition process.

The disclosure materially altered the perceived risk profile of the transaction. Following further assessment, the merger agreement was amended, resulting in a reduction of approximately USD 350 million in the purchase price (Yahoo! Inc. 2017). The adjustment reflected concerns regarding potential legal liabilities, remediation costs, and reputational consequences associated with the inherited cybersecurity weaknesses. The case illustrates how historical security failures can directly influence transaction terms even before post-acquisition integration has fully commenced.

5.3.2 Structural Risk Factors

Although the Yahoo breaches predated the integration phase, the case illustrates how cybersecurity weaknesses can materially influence M&A transactions. In this instance, inadequate disclosure and governance oversight had financial consequences even before full operational consolidation occurred. The episode highlights limitations in due diligence processes and the difficulty of obtaining complete visibility into inherited risk.

From a structural perspective, the case underscores that cybersecurity exposure in M&A is not limited to technical integration challenges. Historical weaknesses in monitoring, governance, and incident reporting can influence transaction dynamics, regulatory accountability, and investor confidence. The SEC's enforcement action against Altaba, formerly Yahoo, reinforced the expectation that cybersecurity risks must be properly disclosed and managed (U.S. Securities and Exchange Commission 2018).

The case underscores that cybersecurity exposure in M&A extends beyond technical integration challenges. Historical weaknesses in monitoring and disclosure can materially influence transaction dynamics and regulatory accountability. The U.S. Securities and Exchange Commission later charged Altaba, formerly Yahoo! Inc., for failing to disclose the breach in a timely manner, reinforcing the governance and disclosure dimension of cybersecurity risk in acquisition contexts (U.S. Securities and Exchange Commission 2018). The episode demonstrates that inadequate cybersecurity oversight can

have consequences not only for integration stability but also for legal and regulatory compliance.

The case also demonstrates the asymmetrical nature of cybersecurity's valuation impact. Weaknesses can reduce transaction value, while evidence of strong security posture does not necessarily generate equivalent premiums. This dynamic supports the interpretation of cybersecurity as a risk containment factor within M&A negotiations rather than a direct value enhancer.

5.3.3 Broader Integration Relevance

While the Yahoo-Verizon case differs from Marriott-Starwood in timing and manifestation, both highlight inherited vulnerability as a central theme. In one instance, vulnerabilities persisted into integration; in the other, historical weaknesses affected transaction valuation and governance expectations. Together, the cases reinforce that cybersecurity risk is embedded in organisational transformation, whether it becomes visible before or after closing.

5.4 Comparative Analysis of the Cases

The Marriott-Starwood and Yahoo-Verizon cases illustrate different manifestations of cybersecurity risk within M&A transactions, yet they reveal recurring structural patterns. Examining them comparatively provides insight into how inherited vulnerabilities, governance practices, and disclosure dynamics interact during organisational transformation.

One common element across both cases is the role of inherited weaknesses. In the Marriott-Starwood breach, vulnerabilities embedded within legacy reservation systems persisted into the integration phase due to incomplete monitoring alignment and delayed governance consolidation. In the Yahoo-Verizon case, previously undisclosed breaches materially influenced transaction valuation and regulatory scrutiny. In both instances, the acquiring organisation assumed responsibility for risk conditions that originated prior to closing.

The timing of risk manifestation differs between the cases. Marriott-Starwood demonstrates operational exposure during integration, where system consolidation and governance transition created conditions in which compromise

could persist. Yahoo-Verizon, by contrast, highlights valuation and disclosure consequences arising from historical cybersecurity failures. Despite these differences, both cases confirm that due diligence may not fully reveal inherited risk, and that governance alignment is critical in both negotiation and integration phases.

Another shared theme concerns visibility and oversight. In the Marriott-Starwood case, insufficient monitoring alignment limited detection capability during early integration. In the Yahoo-Verizon case, incomplete disclosure of cybersecurity incidents affected investor confidence and regulatory response. Both situations underscore the importance of transparent governance and structured oversight in managing cyber risk during organisational change.

The comparison also reinforces the asymmetrical financial impact of cybersecurity. Weak security posture can reduce transaction value or increase post-closing liability exposure, while strong cybersecurity rarely generates explicit premiums. This dynamic aligns with empirical financial research indicating that markets penalise breaches but do not equivalently reward preventative strength (Campbell et al. 2003; Gordon et al. 2011).

Taken together, the cases suggest that cybersecurity risk in M&A is not confined to technical compromise. It intersects with valuation, governance accountability, regulatory enforcement, and organisational stability. Whether manifested through persistent operational exposure or through renegotiated transaction terms, inherited vulnerabilities have tangible consequences. These recurring patterns support the broader argument that integration governance must address structural risk drivers rather than isolated technical weaknesses.

5.5 Implications for Integration Governance

The two cases analysed in this chapter underscore a central argument of the thesis: cybersecurity risk in mergers and acquisitions cannot be effectively managed through reactive remediation alone. Once vulnerabilities are inherited, delayed alignment increases the likelihood that weaknesses become embedded within the merged organisation. Structured integration planning, initiated early and guided by clear governance principles, is therefore essential.

The evidence suggests that visibility and stabilisation should precede deep consolidation. Comprehensive asset inventories help clarify the scope of inherited infrastructure. Early alignment of monitoring systems reduces the probability that transitional blind spots emerge. Harmonisation of identity and access management limits the persistence of excessive privileges or legacy authentication mechanisms. Equally important is governance clarity: responsibility for inherited systems must be explicitly defined to avoid ambiguity during the critical early stages following closing.

The cases also highlight that cybersecurity risk extends beyond technical exposure. In both transactions, weaknesses affected financial outcomes, regulatory scrutiny, and organisational reputation. As such, integration governance must be conceived broadly. It must address not only technical harmonisation but also disclosure practices, compliance obligations, and accountability structures. Managing integration risk therefore requires coordinated oversight across security, legal, compliance, and executive functions from the outset of the post-acquisition period.

Rather than treating cybersecurity as a secondary operational concern, the findings suggest that it should be embedded within the core integration governance framework. This shift from reactive correction to structured sequencing forms the basis for the phased integration model developed in the following chapter.

5.6 Lessons for M&A Integration Practice

The comparative examination of the Marriott-Starwood and Yahoo-Verizon cases reinforces the view that cybersecurity risk in mergers and acquisitions is structurally embedded in the integration process rather than confined to isolated technical errors. Although the cases differ in timing and impact, both reveal recurring governance and oversight challenges that extend beyond their individual contexts.

A central theme across the cases is the persistence of inherited vulnerabilities. In both instances, cybersecurity weaknesses predated the transaction and were not fully identified or resolved before integration advanced. The Marriott-Starwood breach demonstrates how legacy systems, when incorporated

without immediate monitoring alignment, can enable compromise to continue undetected. The Yahoo-Verizon transaction, by contrast, shows that historical breaches-even when disclosed during acquisition-can materially influence transaction risk and valuation. Together, these examples highlight that acquisitions transfer not only assets and capabilities, but also accumulated exposure.

Visibility during transitional phases emerges as another decisive factor. Integration often involves temporary coexistence of systems, staged identity consolidation, and architectural bridging between environments. If monitoring infrastructures and incident response processes are not unified early, detection capability may weaken at precisely the moment when exposure increases. In the Marriott-Starwood case, the absence of comprehensive and consolidated monitoring contributed directly to the prolonged duration of the breach.

Governance clarity also proves critical. Both cases illustrate how weaknesses in oversight structures can delay detection and remediation. Immediately following closing, responsibility for inherited systems must be explicitly defined. Without clear accountability for patch management, access control harmonisation, and monitoring alignment, vulnerabilities may persist. Academic research supports this observation, indicating that integration failures often arise from organisational misalignment rather than purely technical shortcomings (Zhao et al. 2023).

The cases further demonstrate that cybersecurity risk in M&A is not confined to operational compromise. It intersects with financial valuation, regulatory scrutiny, and reputational stability. The Yahoo-Verizon transaction illustrates how disclosure of cybersecurity weaknesses can alter transaction economics, while the Marriott-Starwood breach resulted in regulatory consequences and sustained reputational impact. These outcomes suggest that cybersecurity governance must be incorporated into strategic integration planning from the outset rather than addressed retrospectively.

Viewed collectively, these lessons indicate that integration-phase risk is systemic. It emerges from structural complexity, legacy interdependencies, fragmented oversight, identity misalignment, and transitional governance dynamics. The recurrence of these patterns across distinct cases strengthens the central premise of this thesis: effective post-acquisition integration requires a

structured and phased approach to cybersecurity and data protection governance.

The insights drawn from these cases provide the empirical foundation for the analytical synthesis presented in the following chapter. By connecting documented integration failures with theoretical standards and regulatory frameworks, the thesis proceeds to develop a structured model for managing cybersecurity risk during M&A integration.

6 Analysis and Synthesis

6.1 Introduction

The preceding chapters have established both the structural characteristics of integration-phase cybersecurity risk and the empirical evidence drawn from documented M&A cases. This chapter brings those strands together. The objective here is to synthesise theoretical frameworks, regulatory requirements, and comparative case observations in order to clarify how integration-related vulnerabilities emerge and why they persist.

Rather than reiterating descriptive findings, this chapter seeks to move toward explanation. By examining recurring themes across academic research, governance standards, and documented incidents, it becomes possible to identify the structural drivers that consistently shape integration risk. This analytical synthesis directly addresses the first research question by clarifying which cybersecurity and privacy risks are most characteristic of post-acquisition integration in IT-sector transactions.

At the same time, the synthesis provides the conceptual basis for the phased integration model presented in the following chapter. If integration risk arises from predictable structural conditions, then mitigation must also be structured and sequenced accordingly. The discussion that follows therefore serves as a bridge between empirical observation and governance design.

6.2 Recurring Risk Patterns Across Theory and Cases

A comparative reading of academic research, regulatory frameworks, and the Marriott-Starwood and Yahoo-Verizon cases reveals a set of recurring patterns that extend beyond the specifics of individual transactions. Although the technical details differ, the underlying risk dynamics appear consistently

across contexts. These observations suggest that cybersecurity exposure during integration reflects deeper organisational and architectural conditions rather than isolated incidents

Several risk drivers emerge repeatedly. Inherited vulnerabilities are often embedded in legacy systems that predate the acquisition and remain insufficiently documented or monitored. Identity and access management misalignment frequently accompanies transitional phases in which parallel authentication structures coexist. Monitoring infrastructures may remain fragmented while systems are being consolidated. Governance responsibilities may be redistributed without immediate clarity. At the same time, regulatory obligations under frameworks such as GDPR and NIS2 remain fully applicable, increasing accountability pressure during periods of structural change.

These risk drivers do not operate independently. Instead, they interact in ways that can amplify exposure. For example, incomplete visibility may delay detection of weaknesses originating in legacy systems. Governance ambiguity can slow remediation of identity misalignment. Supply chain dependencies may compound the difficulty of achieving consistent control alignment across merged environments.

The interrelationship among these factors is illustrated in Figure 2. Figure 2 visualises the reinforcing interaction among structural drivers. The circular interdependency reflects that no single factor operates independently; inherited vulnerabilities, identity misalignment, monitoring fragmentation, governance ambiguity, regulatory exposure, and supply chain dependencies collectively amplify integration risk.

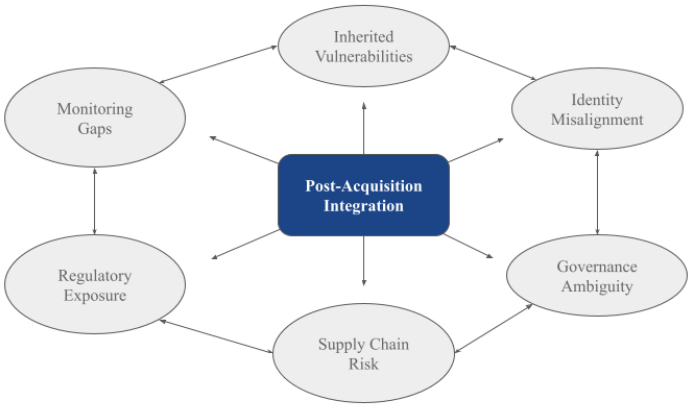

Figure 2. Structural Risk Drivers in M&A Integration

As depicted in Figure 2, integration-related cybersecurity risk arises from the interaction of inherited vulnerabilities, identity misalignment, monitoring gaps, governance ambiguity, regulatory exposure, and supply chain dependencies. The figure emphasises that these drivers reinforce one another rather than functioning in isolation. When combined during transitional phases, they create conditions in which exposure can escalate before governance mechanisms are fully stabilised.

The consistency of these patterns across both empirical cases and scholarly research strengthens the conclusion that integration risk is embedded in the structural complexity of organisational transformation. Recognising this interaction is essential for designing mitigation strategies that address underlying conditions rather than isolated symptoms.

A particularly prominent theme across both cases is the role of inherited vulnerabilities. In the Marriott-Starwood incident, legacy reservation systems with inadequate monitoring and outdated controls were incorporated into the acquiring organisation's environment without immediate and comprehensive oversight (In re Marriott International, Inc. 2021). In the Yahoo-Verizon transaction, previously undisclosed breaches significantly altered transaction dynamics and influenced post-acquisition governance expectations (U.S. Securities and Exchange Commission 2018). Academic research reinforces this pattern, showing that architectural weaknesses and accumulated technical debt materially increase integration risk, especially where compatibility assessments remain incomplete (Zhao et al. 2023). These observations suggest

that due diligence alone cannot eliminate inherited exposure. Integration planning must therefore proceed on the assumption that latent vulnerabilities may exist and should incorporate early stabilisation mechanisms accordingly.

A closely related integration risk concerns the alignment of identity and access management structures. When organisations merge, their authentication mechanisms, directory services, and privilege models are typically designed independently and governed under different control frameworks. Consolidating these structures requires reconciling role definitions, access hierarchies, and administrative oversight while maintaining uninterrupted operations. During transitional periods, temporary permissions are often introduced to facilitate migration activities. If these permissions are not rigorously governed and subsequently reviewed, they may persist beyond their intended duration, increasing exposure. Research on post-merger IT integration indicates that weak alignment between governance mechanisms and system architectures can create persistent integration vulnerabilities, particularly where documentation is incomplete or accountability boundaries are unclear (Wijnhoven et al. 2006; Baker & Niederman 2014). The empirical cases examined in this thesis reinforce that identity fragmentation is not a peripheral concern but a recurring structural condition that can heighten cybersecurity risk when harmonisation is delayed.

Monitoring and visibility represent another area in which transitional instability can amplify exposure. Logging infrastructures may remain partially segregated while integration progresses, and event correlation mechanisms may not yet operate across the entire merged environment. The Marriott-Starwood breach illustrates how insufficiently unified monitoring can allow compromise to remain undetected for extended periods (In re Marriott International, Inc. 2021). Industry analysis similarly notes that organisational change periods often coincide with fragmented detection capability, creating opportunities for exploitation (WTW 2023). Regulatory expectations under NIS2 further emphasise the need for continuous and demonstrable monitoring throughout structural transition (ENISA 2023).

Governance alignment also plays a decisive role. Integration involves redefining roles, reporting lines, and accountability structures across previously separate organisations. Where responsibility for inherited systems is not

clearly allocated, remediation efforts may be inconsistent or delayed. Academic literature consistently identifies governance coordination as a determinant of integration stability (Zhao et al. 2023). In both case studies, weaknesses in oversight structures contributed to elevated exposure, underscoring the importance of early governance consolidation.

Finally, regulatory exposure introduces a further dimension of integration risk. Under GDPR, organisations must ensure lawful processing and appropriate safeguards for personal data regardless of structural change (ICO 2021). During integration, personal data may be consolidated, reclassified, or transferred under new processing contexts. If lawful basis reassessment, controller-processor clarification, and DPIA procedures are not embedded within integration planning, compliance risk increases. The Marriott-Starwood case demonstrates that regulatory accountability follows organisational control, even where vulnerabilities originated prior to acquisition.

Taken together, these patterns confirm that integration risk arises from interdependent technical and governance conditions. Inherited vulnerabilities, identity misalignment, monitoring fragmentation, governance ambiguity, and regulatory exposure interact in ways that can compound one another. Understanding these interconnections is essential for designing mitigation strategies that address structural drivers rather than isolated technical symptoms.

6.3 Structural Drivers of Integration-Phase Risk

The recurring patterns identified in the previous section point toward deeper structural conditions that shape integration-phase cybersecurity risk. These drivers help explain why vulnerabilities intensify during organisational consolidation and why similar issues appear across distinct transactions.

One structural driver is the temporary expansion of system interdependencies. During integration, previously independent technical environments become connected through shared networks, identity frameworks, and data flows. This increased interconnection broadens the potential attack surface. Systems that once operated within contained boundaries may now interact with a larger ecosystem, exposing legacy weaknesses to new threat vectors. As integration progresses, trust relationships between systems are redefined, often before full stabilisation has occurred.

A second driver relates to transitional control instability. Integration rarely unfolds in a single step. Instead, organisations move through phased consolidation, temporary coexistence of systems, and interim governance arrangements. These transitional states can weaken established control baselines. For example, provisional access rights may be granted to facilitate migration, or temporary network bridges may be established to maintain business continuity. Although intended to be short-term solutions, such configurations can persist if not carefully monitored.

Documentation and visibility gaps also contribute structurally to risk escalation. Inherited systems may lack comprehensive architectural documentation or up-to-date asset inventories. Without accurate mapping of system dependencies and data flows, risk assessment becomes less precise. Incomplete documentation complicates the identification of latent vulnerabilities and delays remediation efforts.

Organisational alignment is another critical factor. Integration requires coordination across technical, legal, compliance, and executive functions. Where these units operate under different maturity levels or risk cultures, harmonisation may be uneven. Differences in reporting structures, change management processes, and security practices can slow consolidation. Empirical research on post-merger IS integration demonstrates that failures frequently stem from insufficient coordination and unclear governance structures rather than from purely technical incompatibilities (Henningsson & Carlsson 2011; Baker & Niederman 2014). Integration stability therefore depends not only on architectural compatibility, but also on the capacity of organisational units to operate under a shared governance framework during structural transition.

Strategic pressure further shapes the risk environment. M&A transactions are frequently driven by expectations of efficiency gains, market expansion, or technological advantage. These objectives may compress integration timelines, encouraging rapid consolidation. While operational continuity is essential, accelerated integration can limit opportunities for comprehensive risk assessment. Transitional measures introduced to meet strategic deadlines may become embedded within the merged organisation.

Regulatory obligations intensify these structural dynamics. GDPR and NIS2 impose ongoing accountability regardless of organisational change (ICO

2021; ENISA 2023). During integration, compliance must be maintained even as governance structures evolve. The combination of regulatory pressure and transitional instability increases the complexity of decision-making.

These structural drivers illustrate that integration risk does not stem from isolated technical missteps. It arises from the interaction between expanding system interdependencies, transitional control conditions, documentation gaps, governance realignment, strategic urgency, and regulatory accountability. Recognising these drivers allows integration planning to address root causes rather than surface symptoms.

6.4 Answering Research Question 1

The first research question of this thesis asked: What are the key information security and privacy risks that arise during the post-acquisition integration phase of IT-sector mergers and acquisitions? The synthesis of theoretical frameworks, regulatory requirements, and comparative case analysis allows a structured response.

The evidence indicates that integration-phase cybersecurity risk is multifaceted and interconnected. A primary risk category concerns inherited technical vulnerabilities embedded within legacy systems. These vulnerabilities may include outdated authentication mechanisms, insufficient logging configurations, incomplete patch management practices, and undocumented system dependencies. When such systems are integrated into a broader enterprise environment without immediate stabilisation, exposure increases.

Identity and access management misalignment constitutes a second critical risk dimension. Integration often requires temporary coexistence of multiple identity repositories and phased consolidation of privilege structures. During these transitional periods, inconsistent access controls may persist, increasing the likelihood of excessive privileges or authentication weaknesses. If identity harmonisation is delayed, structural misalignment can remain embedded within the merged environment.

Monitoring and visibility gaps represent another recurring vulnerability. Consolidation of logging infrastructures and SIEM systems typically proceeds in

stages. Until monitoring is unified, detection capability may be uneven. Transitional configurations, such as network bridges or data migration pathways, may not be fully instrumented. Reduced visibility during integration increases the probability that inherited vulnerabilities remain undetected.

Governance ambiguity further amplifies risk. Immediately following acquisition, responsibility for inherited systems must be clearly defined. If accountability for vulnerability remediation, access control alignment, or incident response is unclear, corrective actions may be delayed. Differences in organisational maturity and documentation practices can compound this effect.

Importantly, administrative responsibility extends beyond internal operational ownership to include vendor and third-party governance. Many inherited systems rely on external service providers, cloud platforms, or managed security services. If contractual ownership, escalation authority, or supplier oversight responsibilities remain unclear during integration, remediation efforts may be hindered by ambiguity regarding who is authorised to enforce security obligations or initiate corrective action. Vendor governance is therefore not peripheral to administrative responsibility but a structural component of it.

Regulatory exposure adds an additional layer of complexity. Integration frequently involves reconfiguration of personal data processing activities. Under GDPR, lawful basis reassessment, controller-processor clarification, and security safeguards must be maintained throughout structural change (ICO 2021). NIS2 reinforces leadership accountability and structured risk management obligations (ENISA 2023). Failure to integrate compliance considerations into technical consolidation may result in enforcement action.

Finally, inherited supply chain relationships introduce further risk. Targets may rely on third-party providers whose security posture differs from that of the acquiring organisation. Without systematic reassessment of vendor governance, external dependencies can introduce vulnerabilities into the merged environment.

Taken together, these risk dimensions demonstrate that integration-phase exposure is not the result of isolated technical failures. It reflects the convergence of inherited vulnerabilities, identity misalignment, monitoring fragmentation, governance transition, regulatory accountability, and supply chain

complexity. These factors interact during transitional phases, increasing exposure until governance and control alignment are stabilised.

This synthesis provides a clear and comprehensive answer to the first research question. It also establishes the analytical foundation for addressing the second question: how integration can be structured in phases to manage these recurring risks systematically.

6.5 Transition to the Integration Model

The analysis presented in this chapter has demonstrated that integration-phase cybersecurity risk arises from recurring structural conditions rather than isolated technical events. When inherited vulnerabilities, identity misalignment, monitoring fragmentation, governance transition, and regulatory obligations converge during organisational consolidation, exposure increases in predictable ways.

If these risks are systemic and recurrent, mitigation cannot rely on ad hoc or reactive measures. Instead, integration governance must be deliberately structured and sequenced. Effective risk reduction requires early stabilisation of inherited systems, coordinated alignment of identity and monitoring infrastructures, and clear allocation of accountability throughout the transition.

The following chapter builds upon this analytical foundation by presenting a phased integration model. Grounded in ISO/IEC 27001 and ISO 31000 governance principles, and aligned with GDPR and NIS2 regulatory requirements, the model translates the identified risk drivers into a structured sequence of integration stages. Its purpose is to provide a coherent framework through which organisations can address integration-related vulnerabilities systematically rather than incrementally.

7 A Structured Integration Model for Secure M&A

7.1 Introduction

The preceding chapter demonstrated that cybersecurity risk during post-acquisition integration emerges from recurring structural conditions rather than isolated technical failures. If integration-phase vulnerabilities arise predictably from inherited systems, governance transitions, and regulatory obligations, then mitigation must also be structured accordingly. This chapter translates those analytical insights into a phased integration model designed for IT-sector organisations undergoing M&A consolidation.

The model presented here is not intended as a generic checklist of best practices. Instead, it functions as a governance-oriented framework grounded in the synthesis of academic research, recognised risk management standards, regulatory requirements, and empirical case evidence. It is designed to reflect the reality that integration risk evolves over time. As systems are consolidated, identities aligned, and monitoring infrastructures unified, the organisation's exposure profile shifts. Risk management must therefore follow the progression of integration rather than operate independently of it.

The framework integrates principles derived from ISO/IEC 27001 and ISO 31000 with compliance obligations under GDPR and NIS2. Each phase corresponds to a distinct stage in the transition from inherited complexity to stabilised governance alignment. By sequencing stabilisation, consolidation, harmonisation, and verification, the model addresses the structural risk drivers identified in Chapter 6.

The overall structure of the phased integration model is illustrated in Figure 3. Figure 3 presents the integration model as a stabilisation curve, illustrating how exposure initially increases during structural transition and progressively declines as governance, technical consolidation, and verification mature.

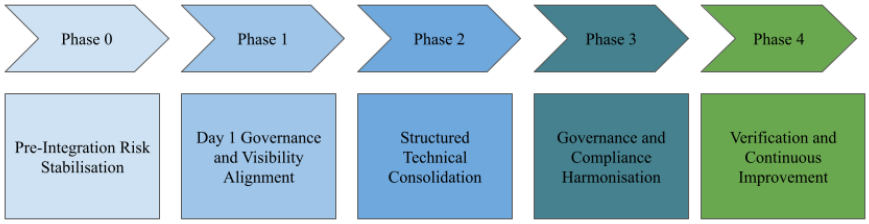

Figure 3. Phased Integration Model for Secure M&A

As shown in Figure 3, the model progresses from pre-integration risk stabilisation through governance and visibility alignment, structured technical consolidation, compliance harmonisation, and ultimately verification and continuous improvement. This progression reflects the dynamic nature of integration-phase risk: exposure initially intensifies during structural transition and gradually stabilises as governance and control alignment mature.

The effect of structured governance sequencing on risk exposure can be conceptually illustrated as shown in Figure 4.

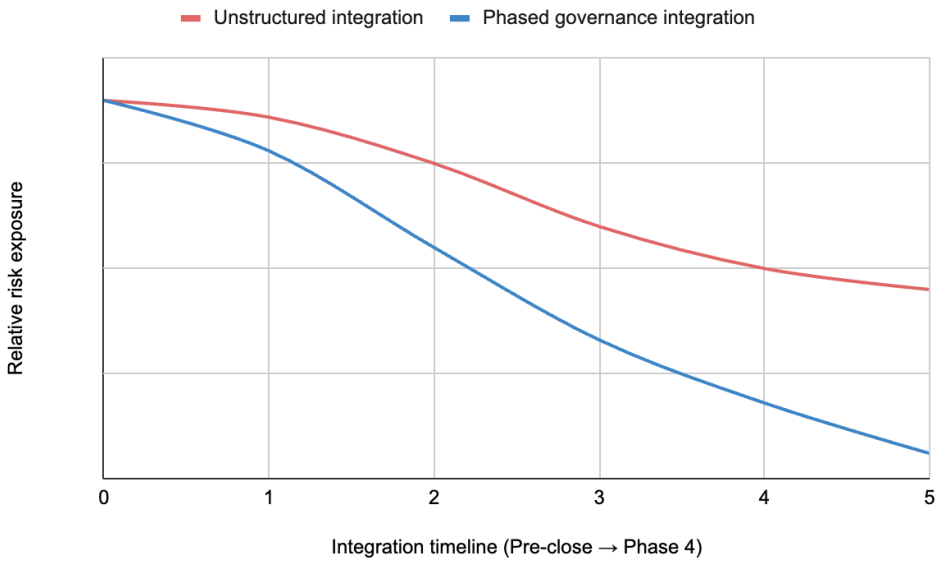

Figure 4. Integration Risk vs Governance Maturity Curve

The figure 4 illustrates how unstructured integration may sustain elevated risk exposure over an extended period, whereas phased governance alignment reduces structural exposure earlier in the integration lifecycle.

The sections that follow examine each phase in greater detail, clarifying its objectives, governance implications, and relationship to the identified risk drivers.

7.2 Phase 0: Pre-Integration Risk Stabilisation

The integration process formally begins at closing, but risk stabilisation should start earlier. Phase 0 addresses the preparatory steps required to reduce uncertainty surrounding inherited systems before operational consolidation intensifies. Its primary objective is to establish visibility and governance clarity so that integration does not proceed without an informed understanding of exposure.

At this stage, acquiring organisations should prioritise comprehensive asset identification and mapping of inherited technical environments. This includes cataloguing applications, infrastructure components, identity repositories, and third-party dependencies. Inherited systems often contain undocumented interfaces and legacy configurations that may not have been fully evaluated during due diligence. Establishing an accurate inventory supports risk assessment and enables prioritisation of stabilisation efforts.

Risk assessment during this phase should be aligned with ISO/IEC 27001 principles, particularly in relation to asset management and control evaluation (Kobayashi et al. 2020). The purpose is not to complete full harmonisation before closing, but to identify high-risk components requiring immediate attention once integration begins. Systems with outdated authentication mechanisms, limited monitoring coverage, or known vulnerabilities should be flagged for early remediation.

Data protection considerations must also be incorporated at this stage. Inherited personal data processing activities should be mapped to ensure clarity regarding lawful basis, processing purposes, and controller-processor rela-

tionships (ICO 2021). Where integration may introduce new processing contexts or expand existing data flows, preliminary assessment of potential GDPR implications helps prevent compliance gaps during subsequent phases.

Leadership involvement is particularly important during Phase 0. Under both ISO governance principles and NIS2 requirements, senior management bears responsibility for ensuring structured cybersecurity risk management (ENISA 2023). Early establishment of accountability for inherited systems reduces ambiguity once operational consolidation begins.

Phase 0 therefore functions as a stabilisation and orientation stage. It acknowledges that inherited exposure cannot be fully eliminated prior to closing, but it ensures that integration proceeds with awareness rather than assumption. By clarifying asset scope, identifying priority risks, and establishing governance responsibility, this phase creates the foundation for disciplined integration in subsequent stages.

7.3 Phase 1: Day 1 Governance and Visibility Alignment

Phase 1 begins immediately following closing. At this stage, ownership has transferred, but full technical consolidation has not yet occurred. The objective is not deep system integration, but stabilisation of governance and visibility. The priority is to prevent inherited vulnerabilities from expanding during the earliest stages of structural alignment.

One of the first tasks in this phase is to establish clear accountability for inherited systems. Roles and responsibilities for monitoring, patch management, vulnerability remediation, and incident response must be explicitly defined. Without early clarification, governance ambiguity can delay risk mitigation and allow exposure to persist. This aligns with ISO 27001's emphasis on defined responsibilities and management commitment (Kobayashi et al. 2020), as well as NIS2's requirement for leadership oversight (ENISA 2023).

Identity and access management requires immediate attention. Privileged accounts should be reviewed, unnecessary access revoked, and temporary migration-related permissions clearly documented. Although parallel identity repositories may remain during transitional periods, access governance must

operate under a unified policy framework. Early enforcement of authentication standards reduces the risk of excessive privilege or legacy credential persistence.

Monitoring alignment is equally critical. Even if full SIEM consolidation cannot be completed immediately, logging pipelines from inherited systems should be connected to central oversight wherever technically feasible. Visibility gaps during this phase increase the likelihood that inherited vulnerabilities remain undetected. The Marriott-Starwood case illustrates how delayed monitoring alignment can allow compromise to persist (In re Marriott International, Inc. 2021).

Segmentation measures may also be appropriate in this phase. Until systems are fully harmonised, maintaining controlled boundaries between environments can reduce the risk of lateral movement. Transitional architectures should be documented, and temporary network bridges clearly governed.

Phase 1 therefore focuses on stabilisation rather than consolidation. By clarifying governance, enforcing baseline access controls, and strengthening visibility, the organisation reduces exposure during the most vulnerable early period following acquisition. This phase acknowledges that structural alignment takes time, but it ensures that risk does not escalate unchecked while integration progresses.

7.4 Phase 2: Structured Technical Consolidation

Phase 2 represents the most technically intensive stage of integration. By this point, governance responsibilities have been clarified and initial visibility stabilised. The focus now shifts to deliberate consolidation of systems, identities, and infrastructure components. The objective is to reduce structural complexity while preserving operational continuity.

Identity harmonisation is typically the first major consolidation task. Parallel directories and authentication mechanisms should be unified under a consistent governance framework. Dormant accounts must be removed, privilege models aligned, and authentication standards standardised. Temporary access

arrangements introduced during earlier phases should be reviewed and withdrawn where no longer necessary. Addressing identity fragmentation at this stage directly mitigates one of the most persistent integration vulnerabilities.

Infrastructure consolidation follows a similar logic. Legacy systems that do not meet the acquiring organisation's security baseline should either be hardened or decommissioned. Patch management practices must be aligned, encryption standards standardised, and segmentation controls reviewed. Consolidation should proceed in defined stages rather than abrupt system merging. Gradual alignment reduces the likelihood that unresolved vulnerabilities are propagated into the broader environment.

Data migration requires careful sequencing. Integration frequently involves merging customer databases, consolidating enterprise resource planning systems, or unifying human resources platforms. Such migrations alter data flows and processing contexts. GDPR principles of data minimisation, purpose limitation, and security of processing must therefore guide migration planning (ICO 2021). Where consolidation introduces high-risk processing activities, structured assessment mechanisms such as DPIAs should be applied.

Monitoring infrastructure should also move toward full unification during this phase. Logging standards should be harmonised, alert thresholds aligned, and incident response processes integrated across environments. Consolidated monitoring ensures that detection capability reflects the newly merged system landscape.

Throughout Phase 2, risk assessment remains iterative. ISO 31000's emphasis on continuous review is particularly relevant as system interdependencies evolve (EY 2023). Technical consolidation changes exposure conditions; reassessment must accompany each structural adjustment.

In practice, however, consolidation rarely occurs under conditions of unlimited resources. Integration teams must prioritise remediation and alignment activities based on risk materiality and systemic impact. Where multiple vulnerabilities or architectural inconsistencies compete for attention, priority should be given to those components that:

1. Expose critical business functions
2. Involve sensitive personal or regulated data
3. Provide privileged or administrative access pathways, or
4. Create lateral movement opportunities across interconnected environments.

This prioritisation reflects ISO 31000's risk-based principle that treatment efforts should be proportionate to potential impact and likelihood. Without explicit prioritisation criteria, integration efforts risk dispersing limited resources across lower-impact tasks while structurally significant exposures remain insufficiently addressed.

Phase 2 therefore aims to transform transitional complexity into coherent architecture. By consolidating identities, infrastructure, data, and monitoring under unified governance, the organisation reduces the structural drivers of integration-phase risk identified earlier.

7.5 Phase 3: Governance and Compliance Harmonisation

By Phase 3, technical consolidation is largely underway or substantially completed. Attention now turns to governance alignment and regulatory harmonisation. While earlier phases focused on stabilisation and structural integration, this stage ensures that policies, procedures, and accountability frameworks reflect the merged organisational reality.

Security governance must be formalised under a unified management structure. Policies inherited from the target organisation should be reviewed and either integrated into or replaced by the acquiring organisation's framework. ISO/IEC 27001 provides guidance on documentation consistency, control standardisation, and internal audit alignment (Kobayashi et al. 2020). Risk registers should be updated to reflect the consolidated environment, capturing residual exposure and new dependencies created during integration.

Data protection governance requires parallel attention. Records of Processing Activities (RoPA) must be revised to reflect reconfigured data flows. Where processing purposes have changed, lawful bases should be reassessed and, if necessary, updated. Privacy notices may require modification to maintain

transparency toward data subjects. If integration has introduced cross-border data transfers, appropriate safeguards must be confirmed (ICO 2021).

Under NIS2, leadership accountability remains central (ENISA 2023). Management must be able to demonstrate oversight of cybersecurity risk management measures within the newly merged organisation. This may involve updating governance committees, clarifying reporting lines, and aligning escalation procedures across business units.

Supplier governance also demands review. Inherited third-party relationships, including cloud providers and managed service operators, should be evaluated against the acquiring organisation's risk standards. Where contractual arrangements are inconsistent with required control maturity, renegotiation or restructuring may be necessary.

Phase 3 therefore addresses the institutional dimension of integration. While earlier phases reduced technical fragmentation, this stage ensures that governance and compliance structures operate coherently within the merged organisation. Without this alignment, technical consolidation alone would not produce sustainable risk reduction.

7.6 Phase 4: Verification and Continuous Improvement

The final phase of the integration model focuses on verification and long-term stabilisation. By this stage, technical consolidation and governance harmonisation have largely been completed. However, integration should not be considered complete until the effectiveness of the new control environment has been systematically evaluated.

Verification involves assessing whether inherited vulnerabilities have been adequately mitigated and whether newly consolidated systems operate under consistent governance. This may include targeted penetration testing, access rights reviews, vulnerability assessments, and incident response simulations. The objective is not only to identify residual weaknesses but also to confirm that monitoring and detection capabilities function across the entire merged environment.

Continuous improvement principles derived from ISO/IEC 27001 are particularly relevant at this stage (Kobayashi et al. 2020). Integration frequently introduces changes that alter risk profiles in subtle ways. Post-integration evaluation provides an opportunity to refine policies, update risk registers, and strengthen documentation practices. Lessons learned during the consolidation process should be formally recorded to inform future transactions.

Regulatory alignment should also be revisited. GDPR compliance mechanisms, including DPIAs and RoPA documentation, should be reviewed to ensure they reflect the stabilised organisational structure (ICO 2021). Under NIS2, leadership must maintain demonstrable oversight of cybersecurity risk management processes (ENISA 2023). Verification therefore includes confirming that governance reporting lines and accountability mechanisms are functioning as intended.

Importantly, Phase 4 recognises that integration is not a discrete event but part of an ongoing governance cycle. The organisation that emerges from consolidation may differ substantially from its pre-acquisition form. Continuous monitoring, reassessment, and improvement ensure that cybersecurity and data protection controls evolve alongside organisational development.

This final phase closes the integration cycle by transitioning from structural alignment to sustained governance maturity. It reinforces the principle that effective integration requires not only consolidation but also verification and institutional learning.

7.7 Answering Research Question 2

The second research question guiding this thesis asked: How can the integration process be structured into practical and sequential phases to ensure systematic management of information security and privacy risks? The phased model developed in this chapter provides a structured response.

The model recognises that integration risk does not remain constant throughout the M&A lifecycle. Exposure evolves as systems are connected, identities consolidated, monitoring infrastructures unified, and governance structures

redefined. Effective mitigation therefore requires sequencing rather than isolated control implementation. By progressing from early stabilisation through technical consolidation and governance harmonisation to verification and continuous improvement, the model aligns risk management activities with the dynamic nature of integration.

Each phase addresses specific structural vulnerabilities identified in Chapter 6. Pre-integration stabilisation focuses on visibility and inherited risk assessment. Early post-closing governance alignment reduces ambiguity and strengthens monitoring continuity. Structured technical consolidation mitigates identity fragmentation and architectural incompatibility. Governance and compliance harmonisation ensure regulatory alignment under GDPR and NIS2. Finally, verification consolidates control maturity and embeds continuous improvement within the merged organisation.

Importantly, the model does not prescribe rigid technical solutions. Instead, it provides a governance-oriented framework adaptable to different acquisition types, including full acquisitions and carve-out transactions. Its purpose is to ensure that integration proceeds deliberately, with risk stabilisation preceding deep consolidation.

Through this structured sequencing, the model transforms the systemic risk patterns identified earlier into manageable governance stages. In doing so, it offers a practical and standards-aligned framework for addressing integration-phase cybersecurity and data protection exposure in IT-sector mergers and acquisitions.

Importantly, the phased integration model is not designed to operate in isolation from broader deal execution processes. Post-acquisition integration typically unfolds through parallel functional tracks, including financial consolidation, human resources harmonisation, commercial alignment, and operational restructuring. Cybersecurity and data protection governance must therefore be embedded within the overall integration programme timeline rather than treated as a standalone technical initiative. If security sequencing diverges from broader integration milestones, remediation efforts risk delay, dilution, or incomplete implementation. By aligning stabilisation, consolidation, and governance harmonisation phases with standard deal governance

structures, the model supports coordinated execution and reduces the likelihood that cybersecurity considerations are subordinated to short-term synergy objectives.

A structured responsibility matrix aligned with the phased integration model is presented in Annex 1 to illustrate governance accountability across integration stages.

8 Conclusions and Future Research

8.1 Summary of Findings

This thesis has examined cybersecurity and data protection risk during the post-acquisition integration phase of mergers and acquisitions in the IT sector. Drawing on academic literature, regulatory frameworks, and comparative case analysis, the study has demonstrated that integration represents a period of heightened structural exposure rather than a neutral operational transition.

The analysis shows that integration-phase risk is driven by recurring and interrelated factors. Inherited technical vulnerabilities, identity and access management misalignment, fragmented monitoring infrastructures, governance ambiguity, regulatory obligations, and supply chain dependencies collectively shape the risk environment. These factors do not operate independently; instead, they interact during transitional phases, amplifying exposure until governance and technical alignment are stabilised.

The comparative examination of the Marriott-Starwood and Yahoo-Verizon cases illustrates that cybersecurity weaknesses can influence both operational outcomes and transaction value. While some risks manifest as persistent compromise during integration, others affect valuation, regulatory accountability, or reputational stability. In each case, inherited exposure became the responsibility of the acquiring organisation.

Through this synthesis, the thesis provides a structured answer to the first research question by identifying the key information security and privacy risks characteristic of integration in IT-sector M&A.

8.2 Contribution of the Thesis

The primary contribution of this study lies in the development of a phased integration model grounded in recognised governance standards and empirical evidence. While prior research has acknowledged the material importance of cybersecurity in M&A transactions, fewer studies have translated this recognition into structured guidance tailored specifically to the integration phase.

By integrating ISO/IEC 27001 and ISO 31000 principles with GDPR and NIS2 regulatory requirements, the model offers a governance-oriented framework for sequencing risk mitigation activities. Rather than proposing isolated best practices, it aligns stabilisation, consolidation, harmonisation, and verification into a coherent progression. In doing so, the model bridges theoretical governance frameworks and practical integration challenges.

The thesis also contributes analytically by framing integration risk as a structural condition emerging from organisational transformation. This perspective moves beyond incident-centric analysis and emphasises systemic drivers embedded within technical consolidation and governance transition.

8.3 Implications for Practice

The findings suggest several practical implications for organisations engaged in M&A activity. First, cybersecurity governance should be integrated into transaction planning from the outset rather than treated as a secondary operational concern. Early visibility into inherited systems and clear allocation of responsibility reduce exposure during the most vulnerable phases.

Second, regulatory alignment must accompany technical consolidation. Compliance with GDPR and NIS2 cannot be postponed until after integration is complete. Instead, lawful processing, documentation updates, and monitoring accountability must be embedded within each stage of transition.

Third, leadership involvement is essential. Governance frameworks emphasise accountability at the management level. Clear oversight structures and documented responsibility reduce ambiguity during transitional phases.

Finally, integration should be approached as a staged process rather than a single consolidation event. Sequencing risk mitigation activities in line with evolving exposure conditions increases the likelihood of stable and secure organisational transformation.

8.4 Limitations

This study relies exclusively on secondary data, including peer-reviewed academic publications, regulatory materials, industry analyses, and publicly documented case evidence. While this approach supports transparency, traceability, and replicability, it limits insight into internal organisational decision-making processes that may not be publicly disclosed. Consequently, certain contextual factors influencing integration outcomes may remain outside the scope of observable evidence.

Although two case studies were examined to support analytical depth and comparative insight, the findings represent analytical generalisation rather than statistical generalisation. The objective of this research was to identify recurring structural patterns and governance dynamics characteristic of integration-phase cybersecurity risk, rather than to quantify the prevalence or probability of such risks across all M&A transactions.

Furthermore, the proposed integration model operates at the governance and structural level. It is designed to provide a standards-aligned sequencing framework rather than detailed technical implementation guidance tailored to specific architectures, technologies, or sector-specific operational environments. Organisations applying the model must therefore adapt its phases to their own technical landscapes, regulatory contexts, and maturity levels.

An additional limitation concerns resource constraints within acquiring organisations. The integration model assumes the availability of sufficient governance attention and operational capacity to execute phased consolidation in a structured manner. In practice, however, information security functions operate alongside ongoing operational demands, incident response obligations, and continuous compliance requirements. M&A transactions frequently alter workload dynamics by introducing additional complexity without proportionate increases in personnel or financial resources. Under such conditions, even well-designed integration frameworks may encounter execution challenges. Competing priorities, limited staffing capacity, and operational “firefighting”

can delay stabilisation efforts or result in partial implementation of governance measures. This practical constraint highlights the importance of organisational capacity planning and suggests that further research should examine how resource allocation models, security programme maturity, and integration governance structures influence the feasibility and effectiveness of structured cybersecurity consolidation.

8.5 Future Research Opportunities

Future research could expand upon this work by examining additional industry sectors or conducting longitudinal studies of post-integration cybersecurity performance. Empirical studies incorporating practitioner interviews could provide deeper insight into decision-making processes during transitional phases and the organisational dynamics influencing integration sequencing.

Further research might also explore how automation, continuous monitoring tools, and AI-assisted risk detection influence integration governance. As digital ecosystems become increasingly distributed and cloud-based, integration risk dynamics may evolve, warranting additional examination.

An additional avenue for future research concerns the international dimension of M&A integration. Cross-border transactions frequently involve differing regulatory regimes, enforcement cultures, and organisational risk appetites. Variations between European regulatory frameworks such as GDPR and NIS2 and governance expectations in jurisdictions such as the United States may create asymmetries in risk perception, disclosure practices, and integration prioritisation. These differences can influence how cybersecurity risk is evaluated, tolerated, or escalated during integration. Comparative studies examining how cross-jurisdictional governance models affect integration outcomes would provide valuable insight into the challenges of aligning security expectations across regulatory and cultural boundaries.

8.6 Final Conclusion

Cybersecurity and data protection risk during M&A integration is not accidental. It arises from the structural complexity of merging heterogeneous digital environments under evolving governance and regulatory constraints. Recognising these dynamics enables organisations to move from reactive remediation toward deliberate, phased risk management.

By synthesising theoretical frameworks, regulatory requirements, and documented case evidence, this thesis has developed a structured model for managing integration-phase exposure. Organisations that approach post-acquisition consolidation through disciplined governance sequencing are better positioned to safeguard operational stability, regulatory compliance, and transaction value.

9 References

Alaranta, M & Henningsson, S 2008, 'An approach to analyzing and planning post-merger IS integration: Insights from two field studies', Information Systems Frontiers, vol. 10, no. 3, pp. 307–319.

Baker, E & Niederman, F 2014, 'Integrating the IS function after mergers and acquisitions: Analysing business–IT alignment', Journal of Strategic Information Systems, vol. 23, no. 2, pp. 112–127.

Bradley, T 2022, 'Marriott Data Breach FAQ: How Did It Happen and What Was the Impact?', CSO Online. Available at: https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html (Accessed: 10 January 2026)

Campbell, K, Gordon, LA, Loeb, MP & Zhou, L 2003, 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', Journal of Computer Security, vol. 11, no. 3, pp. 431-448.

Deloitte 2024, Cyber Risk in Mergers and Acquisitions. Deloitte Insights. Available at: https://www.deloitte.com/ca/en/Industries/tmt/perspectives/securing-your-next-digital-house.html (Accessed: 4 February 2026)

ECGI 2024, M&A and Cybersecurity Risk: Empirical Evidence. European Corporate Governance Institute Working Paper. Available at: https://www.ecgi.global/sites/default/files/Paper%3A%20M%26amp%3BA%20and%20Cybersecurity%20Risk%3A%20Empirical%20Evidence.pdf (Accessed: 15 January 2026)

ENISA 2023, NIS2 Directive. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/topics/nis2-directive (Accessed: 26 January 2026)

Gordon, LA, Loeb, MP & Zhou, L 2011, 'The impact of information security breaches: Has there been a downward shift in costs?', Journal of Computer Security, vol. 19, no. 1, pp. 33-56.

Grant Thornton 2021, Cybersecurity in M&A Strategy. Grant Thornton Advisory. Available at: https://www.grantthornton.com/insights/articles/advisory/2021/cybersecurity-in-ma-strategy (Accessed: 26 January 2026)

Henningsson, S & Carlsson, S 2011, 'The DySIIM model for managing IS integration in mergers and acquisitions', Information Systems Journal, vol. 21, no. 5, pp. 441–476.

ICO 2021, Data Sharing in Mergers and Acquisitions. Information Commissioner's Office (UK). Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/due-diligence/ (Accessed: 10 January 2026)

Information Commissioner's Office 2020, ICO fines Marriott International Inc £18.4 million for failing to keep customers' personal data secure. Available at: https://webarchive.nationalarchives.gov.uk/ukgwa/20201229162312/https:/ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/ (Accessed: 15 January 2026)

In re Marriott International, Inc. Customer Data Security Breach Litigation 2021,19-md-2879 (D. Md. 11 June 2021), United States District Court for the District of Maryland. Available at: https://www.uschamber.com/assets/documents/Opinion20-20In20re20Marriott20International2C20Inc.20Customer20Data20Security20Breach20Litigation2028D.20Md.29.pdf (Accessed: 10 January 2026)

Kamiya, S, Kang, JK, Kim, J, Milidonis, A & Stulz, RM 2018, 'What is the impact of successful cyberattacks on target firms?', Journal of Financial Economics, vol. 129, no. 3, pp. 491-508.

Kobayashi, N, Matsuno, Y & Hasegawa, K 2020, 'Evaluation of Assurance Case Description Method Using ISO/IEC 27001 for M&A', Journal of Information Security. Available at: https://www.researchgate.net/publication/341998828 (Accessed: 21 January 2026)

Reuters 2017, 'Verizon cuts Yahoo deal by $350 million after data breaches'. Available at: https://www.reuters.com/article/technology/verizon-close-to-yahoo-deal-price-cut-of-250-350-million-sources-idUSKBN15U21Q/ (Accessed: 21 January 2026)

U.S. Securities and Exchange Commission 2018, Altaba, Formerly Known as Yahoo! Inc., Charged With Failing to Disclose Massive Cybersecurity Breach. Available at: https://www.sec.gov/news/press-release/2018-71 (Accessed: 10 January 2026)

WTW 2023, Cybersecurity Considerations in Mergers and Acquisitions. Willis Towers Watson. Available at: https://www.wtwco.com/en-gb/insights/2024/08/cybersecurity-considerations-in-merger-and-acquisitions-transactions-an-in-depth-analysis (Accessed: 11 January 2026)

Yahoo! Inc. 2017, Current Report on Form 8-K, filed 21 February 2017. U.S. Securities and Exchange Commission (EDGAR database). Available at: https://www.sec.gov/edgar (Accessed: 26 January 2026)

Wijnhoven, F, Spil, T & Stegwee, R 2006, 'Post-merger IT integration strategies: An IT alignment perspective', Journal of Strategic Information Systems, vol. 15, no. 1, pp. 5–28.

Zhao, Y, Li, X & Wu, H 2023, 'What Makes Information Systems Integration Successful in Mergers and Acquisitions?', Procedia Computer Science, vol. 217, pp. 685-694. Available at: https://www.sciencedirect.com/science/article/pii/S187705092300340X (Accessed: 11 January 2026)

10 Annex 1 - Phase-Based Integration Governance Responsibility Matrix

The following responsibility matrix aligns key governance activities with the phased integration model presented in Chapter 7. The matrix is intended to clarify accountability during post-acquisition integration and to support structured risk management.

It does not represent a universal or prescriptive template. Rather, it illustrates how governance responsibilities may be distributed across organisational functions in a structured integration context.

The precise allocation of roles and responsibilities will depend on factors such as organisational size, structural complexity, regulatory environment, and available resources. Accordingly, the matrix should be interpreted as an adaptable governance reference rather than a one-size-fits-all solution.

R = Responsible (executes the activity)

A = Accountable (ultimate ownership / decision authority)

C = Consulted (provides input)

I = Informed (kept aware)

Table 1 Phase 0 - Pre-Integration Risk Stabilisation

Activity	CISO / Security	IT Operations	Legal / DPO	Executive Management	External Vendors
Inherited asset inventory	C	R	C	A	C
Preliminary risk assessment	R	C	C	A	I
Data processing mapping	C	I	R	A	I
Third-party risk review	R	C	C	A	C
Governance role definition	C	I	C	R/A	I

Table 2 Phase 1 - Day 1 Governance and Visibility Alignment

Activity	CISO / Security	IT Operations	Legal / DPO	Executive Management	External Vendors
IAM privilege review	A	R	C	I	C
Monitoring baseline alignment	R	A	I	I	C
Incident response alignment	A	R	C	I	I
Segmentation / containment measures	A	R	I	I	C
Accountability confirmation	C	C	C	R/A	I

Table 3 Phase 2 - Structured Technical Consolidation

Activity	CISO / Security	IT Operations	Legal / DPO	Executive Management	External Vendors
Identity system harmonisation	A	R	C	I	C
Legacy system hardening	A	R	I	I	C
Data migration security review	C	R	A	I	C
SIEM consolidation	A	R	I	I	C
Vendor security reassessment	R	I	C	A	C

Table 4 Phase 3 - Governance and Compliance Harmonisation

Activity	CISO / Security	IT Operations	Legal / DPO	Executive Management	External Vendors
Policy harmonisation	R	C	C	A	I
Risk register update	R	C	C	A	I
GDPR compliance review	C	I	R	A	I
NIS2 accountability alignment	C	I	C	R/A	I
Supplier contract reassessment	R	C	C	A	R

Table 5 Phase 4 - Verification and Continuous Improvement

Activity	**CISO / Security**	**IT Operations**	**Legal / DPO**	**Executive Management**	**External Vendors**
Post-integration security testing	A	R	I	I	C
Privilege revalidation	A	R	C	I	I
DPIA review (if applicable)	C	I	R	A	I
Governance effectiveness review	R	I	C	A	I
Lessons learned documentation	R	C	C	A	I