POLITECNICO DI TORINO

Master's Degree in Engineering and Management

Master's Degree Thesis

Shadow IT Rationalization in Banking: Persistence Mechanisms, Risk Translation, and the Limits of Technological Governance

Supervisor: ***Prof. Marco Cantamessa***

Candidate: ***Faris D'ottavio***

March 2026

Ringraziamenti

Abstract

Shadow IT—unauthorized information systems developed and operated outside formal governance structures—has evolved from episodic workaround to structural feature of banking technology landscapes, yet organizations struggle to rationalize these informal tools despite repeated modernization efforts. This thesis examines why shadow IT persists in legacy-intensive banking environments and how automation-driven rationalization initiatives reshape rather than resolve underlying governance challenges.

Through action research conducted during a six-month consulting intervention in a major Italian banking institution, the study investigates shadow IT rationalization across four operational domains governing revenue provisioning, contract management, succession workflows, and regulatory reporting. These processes relied on Excel macros and Access databases containing undocumented business logic accumulated over decades. The bank attempted to replace these tools with Appian low-code platforms and Robotic Process Automation as part of a digital transformation program mandated by regulatory compliance and operational continuity imperatives.

Analysis of semi-structured interviews, process-mapping workshops, and intervention observations reveals three interconnected mechanisms. First, shadow IT persists because informal tools function as unacknowledged middleware layers executing critical validation and integration logic absent from rigid legacy systems, whilst simultaneously serving as institutional memory repositories preserving frozen policy that current operators execute but cannot explain. Second, modernization through low-code and RPA constitutes risk reconfiguration rather than elimination: organizations trade operational flexibility and local intelligibility for standardization and audit trails, shifting risks from execution errors to algorithmic rigidity and black-box opacity. Third, rationalization effectiveness depends fundamentally on organizational dynamics rather than technical capabilities—fragmented process ownership, semantic misalignment, and contested accountability structures systematically undermine technology-centric interventions.

The research contributes theoretically by extending path-dependency frameworks to explain shadow IT institutionalization, challenging technological optimism surrounding automation platforms, and establishing that social rationalization—achieved through collaborative visualization and stakeholder negotiation—constitutes a prerequisite for technical rationalization. Practically, findings demonstrate that effective governance in banking digital transformation requires diagnosing structural drivers of shadow IT adoption, explicitly managing risk trade-offs when selecting automation targets, institutionalizing cross-functional alignment mechanisms, and preserving institutional memory through phased migration strategies. Shadow IT rationalization emerges as a socio-technical challenge demanding coordinated transformation of technology, governance structures, and organizational relationships rather than prohibition or replacement alone.

Table of Contents

1.Introduction

1.1 Research Context: Digital Transformation and Shadow IT in Banking

Financial institutions worldwide face unprecedented technological and competitive pressures that demand rapid digital innovation whilst maintaining strict regulatory compliance and operational continuity (Fürstenau et al., 2017). Digital transformation—the strategic integration of digital technologies to fundamentally reshape business processes, customer experiences, and organizational capabilities—has become essential for banks seeking competitive advantage in increasingly digitalized markets (Abildtrup, 2024). Yet this transformation occurs within institutional contexts characterized by legacy systems, fragmented architectures, and accumulated technical debt that constrain organizational agility (Irani et al., 2023).

Shadow IT—information systems, software, or services developed, acquired, or operated by business units without formal IT department approval—has emerged as a persistent organizational response to these tensions (Klotz et al., 2019). Originally conceptualized as episodic workarounds to address temporary IT responsiveness gaps, Shadow IT has evolved into a structurally embedded feature of organizational technology landscapes, particularly within banking where regulatory obligations intensify governance complexity whilst competitive demands accelerate innovation cycles (Fürstenau et al., 2017; Raković, 2020). Evidence suggests that Shadow IT adoption in large enterprises increased from 30–40% of IT spending pre-pandemic to 41% in 2022, with projections reaching 75% by 2027 (Nugraha et al., 2025).

Banking institutions represent a particularly salient context for examining Shadow IT persistence. The sector's dual mandate—stringent regulatory scrutiny alongside competitive innovation imperatives—creates structural conditions that simultaneously discourage unauthorized technology adoption through formal risk management whilst incentivising informal solutions when formal systems fail to meet evolving business needs within acceptable timeframes (Fürstenau et al., 2017). Regulatory frameworks including Basel III, GDPR, MaRisk, and DORA impose substantial compliance obligations and risk-management requirements that increase both the costs of Shadow IT non-compliance and the governance complexity of managing decentralized technology adoption (Fürstenau et al., 2017). Paradoxically, these same regulatory pressures often motivate Shadow IT creation when centralized IT departments lack the domain-specific knowledge, responsiveness, or resources to deliver compliant solutions rapidly enough to meet business demands (Klotz et al., 2019).

1.2 Research Motivation, Objectives and Contribution

Despite growing recognition of Shadow IT's organizational significance, existing research exhibits three critical gaps that this thesis addresses. First, dominant theoretical frameworks emphasize *adoption drivers*—IT unresponsiveness, user empowerment desires, technological consumerization—yet inadequately explain *persistence mechanisms* through which temporary workarounds become institutionalized organizational infrastructure (Klotz et al., 2019; Raković, 2020). Routinization, knowledge embeddedness, substitution failure, and organizational dependency transform Shadow IT from transient deviations into embedded systems that organizations struggle to eliminate despite repeated rationalization efforts (Fürstenau et al., 2017). Theoretical frameworks capable of explaining long-term institutionalization dynamics beyond initial adoption episodes remain underdeveloped.

Second, modernization technologies—particularly automation platforms such as Robotic Process Automation (RPA) and low-code/no-code development environments—are promoted as governed alternatives to Shadow IT that reconcile agility with control (Shah, 2025; Lakkaraju, 2025). Yet emerging evidence suggests these technologies may reproduce or relocate Shadow IT risks across new technological layers rather than genuinely resolving underlying governance tensions (Yeo and Megargel, 2024). The conditions under which automation-based modernization strategies successfully mitigate versus merely reconfigure Shadow IT-related risks remain empirically underexplored, particularly within regulated banking contexts where transparency demands conflict with platform opacity.

Third, Shadow IT rationalization is often conceptualized as a technical or policy challenge addressable through detection tools, governance frameworks, or prohibition strategies (Zimmermann et al., 2014). However, qualitative evidence reveals that organizational silos, weak business-IT relationships, and ambiguous process ownership frequently undermine centralised rationalisation initiatives (Fürstenau et al., 2017; Nugraha et al., 2025). Understanding why formal risk-management programs fail to prevent Shadow IT recurrence requires integrating organizational theory—emphasizing structure, collaboration, and stakeholder dynamics—with IT governance perspectives.

This thesis addresses these gaps through an embedded case study conducted during a six-month internship within a large European bank's digital transformation program. The research investigates Shadow IT persistence mechanisms, automation-platform governance outcomes, and organizational determinants of rationalization effectiveness within a real-world banking context characterized by legacy-system complexity, regulatory pressures, and ongoing digital transformation initiatives.

1.3 Brief Overview of Research Gaps and Questions

Three research questions structure the empirical investigation:

RQ1: *What mechanisms explain Shadow IT persistence and institutionalization within legacy-intensive banking organizations undergoing digital transformation?*

RQ2: *Under what conditions do automation-based modernization initiatives (particularly RPA deployments) successfully mitigate versus reproduce Shadow IT-related governance risks?*

RQ3: *Which organizational structures and stakeholder dynamics determine the effectiveness of Shadow IT rationalization efforts within banking digital transformation projects?*

These questions collectively advance understanding of Shadow IT evolution from episodic behaviour to structural institutionalization, the governance implications of emergent automation technologies, and the organizational conditions enabling successful rationalization within highly regulated, legacy-intensive institutional environments.

1.4 Key Concepts, Definitions, and Brief Theoretical Foundations

Shadow IT denotes information systems, software, or services developed, acquired, or operated outside formal IT governance structures, characterized by absence of central IT knowledge, alignment, or approval (Klotz et al., 2019). Differentiated from *Business-Managed IT* (overt, sanctioned decentralized solutions operating within explicit governance arrangements), Shadow IT remains covert, limiting organizational visibility, coordination, and accountability (Klotz et al., 2019).

Persistence mechanisms—routinization (embedding into workflows), knowledge embeddedness (concentration of expertise within informal systems), substitution failure (formal systems' inability to replicate Shadow IT functionality), and organizational dependency (business process reliance)—explain transitions from temporary workarounds to institutionalized infrastructure (Fürstenau et al., 2017; Raković, 2020).

Legacy systems represent outdated IT architectures containing business-critical data and processes that resist modification due to technical debt, fragmented architectures, and knowledge gaps (Khabouze, 2022; Irani et al., 2023). Within banking, core platforms designed for robustness often lack modularity and adaptability, creating structural conditions favoring Shadow IT emergence when business units require rapid, context-specific solutions (Fürstenau et al., 2017).

Digital transformation encompasses strategic integration of digital technologies to reshape business models, customer experiences, and operational processes (Abildtrup, 2024). Within banking, transformation initiatives confront tensions between innovation imperatives and compliance obligations, often accelerating Shadow IT adoption when formal governance processes cannot accommodate required change velocities (Lakkaraju, 2025).

Automation platforms—including RPA, low-code/no-code development environments, and intelligent process automation—promise governed agility through standardized, centrally managed development capabilities (Shah, 2025; Yeo and Megargel, 2024). Yet configuration-driven nature and dependency on underlying legacy systems may introduce new opacity and governance challenges.

1.5 Thesis Structure

Following this introduction,
Chapter 2 presents a comprehensive literature review synthesizing research on Shadow IT conceptualization, legacy systems, digital transformation, and automation technologies within banking contexts, identifying theoretical gaps motivating the research questions.
Chapter 3 explicates the action research methodology employed during the six-month internship intervention, detailing data collection through semi-structured interviews and process-mapping workshops.
Chapter 4 presents empirical findings organized around the three research questions, documenting Shadow IT persistence patterns, automation governance outcomes, and rationalization dynamics observed within the case organization.
Chapter 5 discusses theoretical contributions to institutional theory and IT governance literature, practical implications for banking practitioners, and methodological reflections on action research in sensitive organizational contexts.
Chapter 6 concludes with synthesis of key insights, practical recommendations, and directions for future research on Shadow IT governance in digitally transforming organizations.

2. Literature Review

This chapter establishes the theoretical foundations underpinning the thesis by synthesizing existing research on Shadow IT, legacy systems, digital transformation, and automation technologies within the banking sector. Rather than presenting isolated studies, this review identifies conceptual convergences and divergences across the literature, highlighting critical gaps that justify the research questions examined in subsequent chapters. The review is organized into nine logically interconnected sections that progressively build from foundational definitions to unresolved theoretical tensions.

2.1 Shadow IT and Business-Managed IT: Clarity and Ambiguities

Shadow IT denotes information systems, software, or services developed, acquired, or operated by business units without the knowledge, alignment, or formal approval of the central IT function (Klotz et al., 2019). The defining characteristic is not decentralization per se, but the absence of formal governance—shadow IT emerges outside established control structures, limiting organizational visibility, coordination, and accountability (Klotz et al., 2019). This distinction becomes critical when differentiating Shadow IT from Business-Managed IT (BMIT), which refers to overtly decentralized IT solutions operating within explicit governance arrangements and shared responsibility models with central IT (Klotz et al., 2019). While both involve business-unit autonomy, Shadow IT remains covert, whereas BMIT is overt and sanctioned (Kopper et al., 2018).

The literature employs a constellation of related terms—workarounds, feral practices, shadow systems, and shadow sourcing—each capturing distinct facets of unauthorized IT activity (Kopper & Westner, 2016; Klotz et al., 2019). Taxonomies classify Shadow IT along dimensions such as novelty (unofficial versus misuse of official IT), artifact type (devices versus applications), infrastructure scope (shadow versus official infrastructure), and organizational scale (individual versus group-level adoption) (Kopper & Westner, 2016). These taxonomies typically characterize Shadow IT as unofficial, application-centric, and embedded in operational outcomes rather than formal design processes (Kopper & Westner, 2016).

Despite conceptual clarity along governance and artifact dimensions, a critical gap concerns temporal scope. Most definitions treat Shadow IT as episodic or transient, implicitly assuming that once detected or addressed, it disappears (Klotz et al., 2019). However, empirical observations reveal that Shadow IT frequently persists and becomes institutionalized within organizations (Fürstenau et al., 2017; Raković, 2020). This persistence cannot be adequately explained by traditional adoption drivers—IT responsiveness failures, user empowerment desires, or technological consumerization—that dominate existing frameworks (Klotz et al., 2019; Zimmermann et al., 2017).

The mechanisms through which informal systems transition from temporary workarounds to embedded organizational infrastructure—routinization, knowledge embeddedness, substitution failure, and organizational dependency—remain insufficiently theorized

(Fürstenau et al., 2017; Raković, 2020). Routinization refers to the embedding of Shadow IT into daily workflows and tacit knowledge practices, such that formal alternatives appear disruptive or costly to adopt (Raković, 2020). Substitution failure occurs when formal systems cannot replicate the flexibility or procedural logic embedded in Shadow IT, creating path dependency over time (Raković, 2020). Knowledge embeddedness describes the concentration of domain expertise and decision logic within Shadow IT artifacts, often undocumented and maintained by a small number of individuals, making systems opaque to successors (Fürstenau et al., 2017). Organizational dependency emerges when business processes and downstream systems become reliant on Shadow IT for continuity, even when triggering conditions change (Fürstenau et al., 2017).

These persistence mechanisms transform adoption drivers into continuation drivers, yet extant research has not systematically explored their interplay, particularly in regulated, legacy-intensive environments such as banking (Klotz et al., 2019; Raković, 2020). This temporal gap motivates a shift in analytical focus from why Shadow IT emerges to why Shadow IT endures.

2.2 Shadow IT's Transformation: From Ad Hoc Solutions to Organizational Lock-In

Early Shadow IT research, encompassing systematic reviews of over 100 studies, concentrated on antecedents until approximately 2015, focusing on individual behavior, technological opportunities, and business-IT misalignment (Klotz et al., 2019). Shadow IT was predominantly framed as an episodic response to local inefficiencies rather than a recurring organizational pattern (Klotz et al., 2019). From 2016 onwards, scholarly attention shifted toward governance-oriented questions—detection, assessment, and instance-level management—reflecting recognition that Shadow IT is structurally embedded rather than solely user-driven (Klotz et al., 2019; Zimmermann et al., 2014).

Post-2018 studies, particularly those responding to the COVID-19 pandemic, have emphasized temporal dynamics more explicitly. Nugraha et al. (2025) report that Shadow IT adoption in large enterprises increased from an estimated 30–40% of IT spending pre-pandemic to 41% in 2022, with projections suggesting it may reach 75% by 2027. Pandemic-era research documents how emergency workarounds deployed for remote work and crisis response remained embedded after the immediate crisis subsided (Nugraha et al., 2025). This trajectory indicates that Shadow IT has shifted from isolated user experimentation to a pervasive structural feature of organizational technology landscapes (Nugraha et al., 2025).

Despite this evolution, the literature remains analytically proximate to the moment of adoption. Explanations for why informal systems persist beyond their original creators are comparatively underdeveloped (Klotz et al., 2019; Fürstenau et al., 2017). Raković's (2020) systematic review highlights that Shadow IT frequently originates as gap-filling responses to ERP or core system limitations and subsequently evolves toward partial or complete replacement roles, especially when formal systems fail to adapt. Similarly, Fürstenau et al. (2017) observe that in banking contexts, Shadow IT often supports core processes rather than

peripheral activities, and its persistence reflects accumulated operational dependence rather than opportunistic policy deviation.

This distinction between adoption drivers and persistence mechanisms implies that a purely adoption-centric framework is insufficient. Explaining persistence requires attention to structural and historical conditions—technical debt, fragmented architectures, knowledge distribution, and power dynamics—that lock informal systems in place even when original incentives change (Klotz et al., 2019; Fürstenau et al., 2017). Path dependency theory and institutional theory offer promising lenses for analyzing how technical decisions, organizational routines, and knowledge distributions create lock-in that persists despite managerial intentions to rationalize (Berente et al., 2008; Azad & King, 2012).

2.3 Shadow IT in Banking Contexts

Banking institutions face a distinctive structural tension: stringent regulatory scrutiny mandates compliance rigor and operational continuity, while competitive pressure demands rapid digital innovation and customization (Fürstenau et al., 2017). This dual mandate increases the likelihood that business units adopt informal technological solutions when formal systems cannot meet evolving needs within acceptable timeframes or costs (Fürstenau et al., 2017).

A qualitative case study of a German savings bank illustrates how these conditions foster Shadow IT and shape its persistence (Fürstenau et al., 2017). Trading and treasury units developed shadow systems to compensate for limitations in official infrastructure, particularly where central IT lacked domain-specific business knowledge and could not respond with sufficient speed (Fürstenau et al., 2017). The study identifies a governance-problem cycle in which distant business-IT relationships, cost pressures, and diversification demands encourage shadow system creation; as these systems grow and become operationally critical, power relations shift toward business units, reducing central IT's ability to enforce standards and maintain architectural coherence (Fürstenau et al., 2017).

Regulatory interventions then trigger a decommissioning cycle: new risk-management obligations—such as German MaRisk rules—lead senior management and central IT to construct shadow systems as risks and pursue recentralization through risk assessments, system inventories, and integration or replacement attempts (Fürstenau et al., 2017). However, the case reveals that decommissioning efforts often fail to eliminate Shadow IT when underlying causes—lack of shared business knowledge, weak trust, and structural distance—remain unaddressed (Fürstenau et al., 2017). New shadow systems continue to emerge even while others are being decommissioned, resulting in an IT landscape characterized by persistent informality (Fürstenau et al., 2017).

This evidence suggests that in banking, Shadow IT frequently supports core processes rather than peripheral activities, and its persistence reflects accumulated operational dependence and embedded knowledge, not merely opportunistic deviations from policy (Fürstenau et al., 2017). The feedback loop between governance problems and decommissioning cycles highlights that risk construction itself becomes a power-shifting mechanism, enabling central

IT to regain control temporarily without necessarily addressing root causes (Fürstenau et al., 2017).

Raković's (2020) systematic review corroborates this pattern, noting that Shadow IT in regulated sectors often begins as gap-filling but evolves toward replacement roles when formal systems fail to adapt, creating de facto infrastructure that organizations cannot easily replace. The German bank case illustrates that regulatory frameworks—such as MaRisk, GDPR, Basel III, and DORA—increase both the cost of non-compliance and the governance complexity of managing Shadow IT, yet fail to prevent its recurrence if structural business-IT misalignment persists (Fürstenau et al., 2017).

2.4 Drivers of Shadow IT Adoption: Enablers, Motivators, and Missing Barriers

The literature commonly groups Shadow IT adoption factors into three categories: enablers, motivators, and missing barriers (Klotz et al., 2019). Enablers reduce the effort required to deploy IT autonomously—cloud services, end-user development platforms, and increasing digital competence among employees facilitate Shadow IT creation without requiring traditional IT department involvement (Klotz et al., 2019; Kopper et al., 2018). Motivators are organizational shortcomings: slow IT response times, inflexible architectures, limited domain understanding within central IT, and business-IT misalignment drive business units toward autonomous solutions (Klotz et al., 2019; Raković, 2020). Missing barriers include weak enforcement, unclear policies, and cultural tolerance for informal solutions during periods of rapid change (Klotz et al., 2019).

While these factors explain why Shadow IT emerges, they only partially explain why it becomes operationally critical and enduring. Fürstenau et al. (2017) show that cost pressures, product diversification needs, and distant business-IT relationships that initially motivated shadow system creation were not resolved by later policy interventions; once systems were embedded in core processes and supported by local expertise, organizations faced new challenges of substitution and migration. Similarly, Raković's (2020) systematic review highlights that many Shadow IT instances originate as gap-filling responses to ERP or core system limitations and later evolve toward partial or complete replacement roles, especially when formal systems fail to adapt.

A convergence emerges across studies: adoption drivers (e.g., IT unresponsiveness, user empowerment) explain initial emergence, but persistence drivers (e.g., routinization, knowledge embeddedness, organizational dependency) explain long-term institutionalization (Klotz et al., 2019; Fürstenau et al., 2017; Raković, 2020). This distinction implies that a purely adoption-centric framework is insufficient—explaining persistence requires attention to structural and historical conditions such as technical debt, fragmented architectures, knowledge distribution, and power dynamics that lock informal systems in place even when original incentives change (Klotz et al., 2019; Fürstenau et al., 2017).

Recent pandemic-era research extends this framework by documenting a motivational shift from convenience-driven use (pre-pandemic) to necessity-driven adoption (during crisis) to hybrid-work optimization (post-pandemic) (Nugraha et al., 2025). This temporal evolution suggests that Shadow IT drivers are context-dependent and crisis-sensitive, requiring adaptive governance frameworks that account for changing organizational priorities (Nugraha et al., 2025).

2.5 Consequences of Shadow IT: the Transition from Asset to Liability

Shadow IT delivers well-documented local benefits: increased productivity, better task-technology fit, and greater flexibility in adapting to evolving requirements (Klotz et al., 2019; Raković, 2020). These benefits are particularly salient in environments where formal systems cannot be changed quickly or where local innovation is critical to performance (Kopper et al., 2018). However, over time, the accumulation of shadow systems generates systemic risks. Case studies and surveys report fragmented data models, redundant or conflicting functionality, uncoordinated security practices, and opaque ownership structures as Shadow IT proliferates (Silic & Back, 2014; Zimmermann et al., 2017).

In banking, continuity risks become especially acute when critical shadow systems are known and maintained by only a few individuals and lack documentation—a dynamic captured in the "hit-by-a-bus" scenario, where the departure of key staff threatens business continuity (Behrens, 2009; Fürstenau et al., 2017). The transition from local asset to organizational liability is driven less by the inherent properties of individual tools than by their cumulative interaction. A single spreadsheet macro may pose minor risk; dozens of interconnected, undocumented shadow systems supporting regulatory reporting and trading activities create significant exposure to error, fraud, and compliance failure (Silic & Back, 2014; Panko, 2006).

Pandemic-era studies show how emergency tools introduced to support remote work and crisis operations remained integrated into core processes afterward, often without formal evaluation or rationalization, compounding legacy complexity (Nugraha et al., 2025). Nugraha et al. (2025) report that Shadow IT adoption increased from 30–40% pre-pandemic to 41% in 2022, with projections suggesting 75% by 2027, indicating that crisis-driven adoption patterns have durable effects on organizational IT landscapes.

The risk profile of Shadow IT shifts over time. Initially, risks are primarily technical—data loss, security vulnerabilities, lack of backups (Silic & Back, 2014). As systems accumulate and become embedded, risks become organizational—continuity threats, regulatory non-compliance, architectural fragmentation, and loss of strategic coherence (Zimmermann et al., 2017; Fürstenau et al., 2017). This temporal progression implies that governance interventions must be lifecycle-aware, addressing not only initial adoption but also long-term institutionalization and rationalization challenges (Raković, 2020).

2.6 Legacy Systems, Technical Debt, and Knowledge Embeddedness

Legacy systems form a structural backdrop that both encourages Shadow IT creation and reinforces its persistence (Khabouze, 2022). Core banking platforms are designed for robustness and security but often lack modularity and adaptability; accumulated technical debt makes changes slow and expensive (Khabouze, 2022). In this context, informal solutions become pragmatic responses to misalignment between rigid core systems and dynamic business needs, particularly where business units can rapidly prototype and deploy tools outside central IT processes (Fürstenau et al., 2017; Klotz et al., 2019).

Khabouze's (2022) doctoral study identifies collaboration, documentation, and upskilling as critical strategies for legacy modernization in healthcare and finance, yet notes that organizations frequently struggle to balance modernization with operational continuity. Technical debt—defined as the implied cost of additional rework caused by choosing expedient solutions over robust architectural approaches—accumulates when organizations defer modernization, creating path dependencies that make future changes progressively more difficult (Monaghan et al., 2018; Khabouze, 2022).

A complementary dynamic involves knowledge embeddedness and organizational dependency. Shadow systems frequently codify specialized domain knowledge, regulatory interpretations, and local workflows developed by subject-matter experts; documentation is limited, and understanding resides largely in tacit knowledge (Fürstenau et al., 2017). When these experts leave or their roles change, successors inherit opaque systems they may be reluctant to modify, reinforcing substitution failure (Raković, 2020). Studies of spreadsheet-based solutions and "feral" systems show similar patterns: users trust and rely on tools they have created themselves, even when these tools are technically fragile or non-compliant (Behrens, 2009; Silic & Back, 2014).

As a result, persistence reflects historical accumulation and substitution failure rather than ongoing dissatisfaction with central IT. Shadow IT becomes an institutionalized outcome of organizational constraints—technical, structural, and epistemic—rather than a transient deviation (Fürstenau et al., 2017; Klotz et al., 2019). This reframing has implications for rationalization strategies: efforts that address only technical integration or policy enforcement are unlikely to be effective if they do not also confront embedded knowledge structures and process dependencies (Fürstenau et al., 2017; Raković, 2020).

2.7 Regulatory Governance in Banking: Compliance Paradoxes and Real Control

In banking, regulatory frameworks increase both the cost of non-compliance and the minimum governance standards that technological solutions must meet (Panko, 2006; Zimmermann et al., 2017). Data protection regimes such as GDPR require transparency, lawful processing, and auditable access control; operational-risk and model-risk rules under Basel III and similar frameworks demand documented logic, validation, and traceability for automated decision-making (Panko, 2006; Zimmermann et al., 2017). Shadow IT that

processes personal or risk-relevant data outside sanctioned platforms inherently struggles to satisfy these requirements and therefore heightens compliance risk (Silic & Back, 2014).

Digital Operational Resilience Act (DORA) and equivalent regimes further emphasize ICT risk management, system inventorying, resilience testing, and third-party oversight. These obligations presuppose a comprehensive view of the IT asset landscape, which unmanaged shadow systems undermine (Spivey & McIlveene, 2024). However, research on Business-Managed IT suggests that decentralization is not inherently incompatible with regulatory expectations: when decentralized solutions are overt, inventoried, and governed within agreed frameworks, they can provide agility while still enabling appropriate controls (Klotz et al., 2019; Kopper et al., 2018).

This regulatory context creates a compliance-versus-control paradox. Organizations can implement formal governance mechanisms—approval workflows, access controls, audit logging, and standardized development lifecycles—that produce evidence of compliance for regulators and auditors. Yet formal compliance does not guarantee substantive control when underlying logic is opaque, platform dependencies are poorly understood, or governance structures lack the capacity to scrutinize complex, model-driven systems. The challenge is particularly pronounced for modernization technologies such as automation platforms, which promise to reconcile agility with control but may introduce new forms of opacity and dependency.

Spivey and McIlveene's (2024) comprehensive framework for managing Shadow IT in regulated environments emphasizes anticipation, identification, and adaptive management, advocating for multilayered detection methods, shadow IT reporting systems, and flexible IT policy frameworks rather than prohibition-based approaches. Their research suggests that effective governance in regulated sectors requires balancing risk mitigation with innovation enablement, acknowledging that outright prohibition may drive Shadow IT further underground without addressing root causes (Spivey & McIlveene, 2024).

2.8 Modernization Technologies: Solving or Shifting Governance Problems?

Automation technologies such as robotic process automation (RPA) are often presented as structured responses to Shadow IT, designed to provide speed and flexibility within standardized, centrally governed environments. In banking, these technologies are used to build customer-facing applications, automate back-office workflows, and orchestrate end-to-end processes while ostensibly maintaining visibility and compliance (Shah, 2025).

Empirical studies report substantial efficiency gains. RPA deployments in digital financial services have been shown to reduce transaction processing times by 55–70%, cut compliance errors by 40–70%, and achieve cost savings of 58–64% in selected processes (Shah, 2025). However, research highlights governance ambiguities. The configuration-driven nature of RPA and reliance on user-interface scripts tie bots closely to underlying legacy systems, such

that changes in screens or workflows can cause failures that propagate errors quickly if governance and monitoring are weak (Shah, 2025).

Quantitative evidence from mixed-methods studies underscores the paradox. Shah's (2025) regression models show that governance maturity and AI integration are strong predictors of compliance error reduction in RPA deployments, with higher governance scores associated with significantly fewer regulatory incidents; however, the same models find no statistically significant relationship between governance variables and cost savings, suggesting that financial benefits depend on context-specific factors such as labor costs, process selection, and automation scope (Shah, 2025).

These findings suggest that modernization technologies shift where and how shadow-IT-like risks manifest rather than eliminating them. Agility is delivered through abstraction, configuration, and integration; opacity, dependency, and knowledge gaps move from spreadsheet-based workarounds into platform-specific ecosystems whose risks are harder to detect and manage without specialized expertise (Shah, 2025). Formal compliance may be easier to demonstrate, but substantive control depends on how governance structures, technical skills, and organizational incentives are configured around these tools (Shah, 2025).

2.9 Organizational Dynamics and Rationalization: From Integration to Negotiation

Shadow IT rationalization efforts often assume that the main obstacles are technical or policy-related: lack of inventories, weak controls, or insufficiently strict enforcement (Klotz et al., 2019; Zimmermann et al., 2014). Empirical work in banking suggests that organizational dynamics—particularly structural fragmentation, trust, and process ownership—are equally, and sometimes more, important (Fürstenau et al., 2017; Raković, 2020).

The German bank case shows that formal risk-management programs, including system registries, policy updates, and efforts to centralize ownership, did not prevent the continued emergence of shadow systems when business-IT relationships remained distant and central IT lacked credibility as a partner (Fürstenau et al., 2017). Shadow systems were attractive not only because of their technical characteristics but because they were embedded in business units that felt central IT was unresponsive or unable to understand their needs; decommissioning or centralization was experienced as a loss of control rather than risk mitigation (Fürstenau et al., 2017).

Post-pandemic reviews of Shadow IT governance report a broader shift from prohibition-centric strategies toward more collaborative models (Nugraha et al., 2025). Before the pandemic, the dominant response in many organizations was restrictive: banning certain tools and enforcing compliance through monitoring and sanctions (Nugraha et al., 2025). After the widespread reliance on informal solutions during remote work, a significant share of organizations moved toward discovery-and-dialogue approaches that treat Shadow IT as a source of information about unmet needs and involve business stakeholders in evaluation and

prioritization; studies find that such collaborative models are associated with higher project success rates and faster time-to-market for digital initiatives (Nugraha et al., 2025).

Independent research on automation adoption in banking reinforces the importance of cross-functional collaboration. Interviews with banking professionals show that hybrid teams combining business domain experts, IT architects, and compliance specialists are better able to select appropriate use cases, manage vendor relationships, and ensure that automated solutions align with both regulatory and operational priorities. Organizations with formalized cross-functional structures—such as automation centers of excellence—report lower failure rates in RPA projects and greater ability to scale beyond pilots (Herm et al., 2023; Shah, 2025).

These findings indicate that rationalization effectiveness depends not only on the presence of governance policies and technical tools but also on organizational structures, decision-making authority, and stakeholder alignment. When process ownership is fragmented across multiple units with divergent incentives, central rationalization initiatives may be perceived as externally imposed and face resistance; conversely, when end-to-end process ownership is clear and business units share accountability with IT and risk functions, rationalization can be framed as a joint effort to reduce complexity and risk while preserving local value (Fürstenau et al., 2017; Nugraha et al., 2025).

Spivey and McIlveene (2024) propose a comprehensive framework emphasizing shadow IT governance committees, flexible IT policy frameworks, and multilayered detection methods, arguing that effective management requires balancing control with understanding of employee motivations. Their framework advocates for fostering a culture of transparency and trust that encourages employees to disclose Shadow IT use, providing valuable insights into limitations of existing IT solutions and helping to refine official offerings (Spivey & McIlveene, 2024).

2.10 Unresolved Tensions and Research Opportunities

The literature reviewed in this chapter establishes Shadow IT as a widespread, structurally recurring phenomenon, particularly in regulated and legacy-intensive environments such as banking. Research has clarified core definitions, identified adoption drivers, and catalogued governance responses, but it also reveals three unresolved tensions that motivate the research questions for this thesis.

First, a theoretical tension: Shadow IT persistence is
empirically observed but remains insufficiently theorized as a long-term, path-dependent phenomenon. While adoption drivers have been catalogued, the mechanisms through which informal systems become institutionalized—routinization, knowledge embeddedness, substitution failure, and organizational lock-in—have not been systematically integrated into theoretical frameworks (Klotz et al., 2019; Fürstenau et al., 2017; Raković, 2020). Institutional theory and path-dependency perspectives offer promising lenses for analyzing how technical decisions, organizational routines, and knowledge distributions create lock-in that persists even when management intends to rationalize (Berente et al., 2008; Azad & King, 2012).

Second, a modernization tension: Automation platforms are adopted as mechanisms to mitigate Shadow IT by providing governed agility, yet evidence shows that they can reproduce or relocate risks related to opacity, dependency, and governance capacity (Shah, 2025). The conditions under which these technologies genuinely reduce governance risk versus simply reconfiguring it across new technological and organizational layers remain underexplored. This tension is particularly acute in banking, where regulatory compliance demands transparency yet modernization platforms often introduce proprietary, opaque logic (Shah, 2025).

Third, an organizational dynamics tension: Shadow IT rationalization is often conceptualized as a technical or policy challenge, but empirical studies reveal that silos, weak cross-functional collaboration, and ambiguous process ownership frequently undermine rationalization efforts (Fürstenau et al., 2017; Nugraha et al., 2025; Zimmermann et al., 2017). Understanding rationalization effectiveness, particularly in banking digital-transformation projects, therefore requires integrating organizational theory—focusing on structure, incentives, and collaboration—with IT-governance and technology perspectives (Fürstenau et al., 2017; Nugraha et al., 2025).

These tensions motivate the thesis's three research questions (RQs), which focus on:

1. *The mechanisms through which Shadow IT becomes persistent and institutionalized;*
2. *The governance outcomes of automation-based modernization and the conditions under which it mitigates or reproduces shadow-IT-related risks; and*
3. *The organizational structures and stakeholder dynamics that shape the success or failure of Shadow IT rationalization in banking digital-transformation initiatives.*

3. Research Methodology

The purpose of this chapter is to present and justify the methodological choices adopted to address the three research questions, given the ex-post nature of a study grounded in an internship-based intervention in a large European bank. The chapter explains how an action-research stance, supported by semi-structured interviews and process-mapping workshops, was used to surface organizational mechanisms underlying shadow IT persistence, modernization, and rationalization in a highly regulated, legacy-intensive context.

3.1 Research Approach: Ex-Post Action Research

This thesis adopts an action research approach in which knowledge production and practical intervention are intertwined rather than separated (Staron, 2025; Bleijenbergh et al., 2020). Shadow IT is not a visible category in dashboards or inventories, but is embedded in everyday routines, undocumented workarounds, and legacy practices that typically become salient only when someone attempts to change them. Studying such phenomena therefore requires direct participation in organizational processes (Staron, 2025; Bleijenbergh et al., 2020).

The action research design is ex-post and reflective: the six-month internship project was not originally conceived as an academic study, but as a consulting engagement aimed at mapping, analyzing, and rationalizing shadow IT across selected operational domains. The research was subsequently constructed through systematic reflection on this real organizational intervention, using project activities as a source of empirical material and as occasions to interrogate underlying mechanisms. This positioning is methodologically legitimate in action research, where researchers often enter ongoing change programs with predefined roles and then re-frame their experience analytically (Staron, 2025; Bleijenbergh et al., 2020).

The thesis does not present the project as a linear problem-solving exercise, but as an empirical exploration conducted through action. Interventions such as process-mapping workshops, to-be design sessions, and automation scoping meetings were treated as deliberate probes that made hidden assumptions and tensions discussable. Episodes of resistance, scope disputes, and negotiation deadlocks were treated as core empirical material, consistent with action research traditions that view organizational frictions as sources of insight into deeper structures and power relations (Staron, 2025; Bleijenbergh et al., 2020).

The interventionist stance inevitably shaped the situations being observed. The study therefore adopts an explicitly reflexive attitude, recognizing that the mechanisms developed in Chapter 4—operational dependency and embedded logic, shadow IT as institutional memory, modernization as risk translation, and rationalization as negotiation—emerged progressively through iterative engagement with the cases rather than being prespecified (Dubois & Gadde, 2002).

3.2 Research Design and Case Selection

3.2.1 Qualitative, Single-Case, Abductive Study

The research design is a qualitative, single-case study embedded in an ex-post action research setting. A single banking institution is examined in depth, with multiple operational domains treated as embedded sub-cases. This design is appropriate when the objective is to build a rich understanding of intertwined organizational and technological dynamics in context (Bryman, 2012; Yin, 2009).

Analytically, the study follows an abductive strategy, moving iteratively between empirical material and theoretical concepts from the literatures on shadow IT, IT governance, and digital transformation (Dubois & Gadde, 2002). Existing concepts are used as sensitizing devices rather than as fixed coding templates, in line with "systematic combining" approaches that progressively refine both the empirical focus and the conceptual framework through repeated matching between theory and reality (Dubois & Gadde, 2002). The aim is to identify generative mechanisms that can account for recurrent patterns observed across processes and stakeholder groups (Bryman, 2012; Guest et al., 2011).

Sampling is theoretical and convenience-based: the bank and selected domains were chosen because the internship provided deep access to a typical large, regulated, legacy-intensive banking environment undergoing automation-driven transformation. Generalization is analytical, not statistical: the contribution lies in refining and extending concepts such as shadow IT persistence and modernization-as-risk-translation (Yin, 2009; Bryman, 2012).

3.2.2 Case Bank and Empirical Domains

The case organization is a major Italian banking institution operating under stringent regulatory requirements, a complex landscape of legacy core systems—particularly the CAD accounting platform—and a strategic push toward digital transformation. The bank's transformation program relies heavily on low-code platforms (notably Appian), Robotic Process Automation, and workflow orchestration as key levers for improving governance, efficiency, and traceability.

The banking and financial services sector offers particularly suitable conditions for studying shadow IT and automation-driven modernization, characterized by high transaction volumes, strict compliance demands, complex data reconciliations, and multi-system interactions. The bank is representative of this context: approximately 21 legal entities within the group, multiple operational tribes with distinct product portfolios (savings and investment, day-to-day banking, wealth management, insurance), and external service providers managing portions of critical processes.

The study follows four operational domains where informal systems play a central role:

GESPRO (revenue provisioning and product census): A monthly process managing calculation and reconciliation of commissions owed to asset managers. The process relies on

Excel spreadsheets with VBA macros and terminal emulation software to mediate between the CAD accounting system and business units, orchestrating forecast calculations, reconciling actuals, and automating data entry when variances are within tolerance. The shadow IT application executes validation routines, enforces date rules, checks codes, and handles exceptions—logic accumulated over years and known only to a small number of operators.

Platform Server (contract management): An Access-based application used by the Governance Accounting office to manage inter-company contracts, track effort allocation across 24 contracts and 21 group entities, calculate cost allocations using FTE rates and markup parameters, and prepare quarterly invoicing. The tool maintains service catalogues, tracks contract renewals, and supports both internal services and third-party outsourcing.

Succession processes: Historically supported by an Access database functioning as an operational diary and trigger mechanism for dossier closure. Following partial migration to Appian for specific workflows, the database is no longer maintained, yet a process gap remains around systematic closure of title dossiers, creating risks of premature closures or dependencies on external vendor robots.

Sub-certification (quarterly compliance reporting): A quarterly reporting obligation toward the parent group covering multiple reconciliation quadrants. The process aggregates data from multiple systems, applies manual lookups, formats outputs for submission to Finance, and supports regulatory filings. Multiple macros, local databases, and daily reconciliation routines support this activity, with significant manual effort and fragile integration points.

These domains exhibit the full spectrum of shadow IT characteristics: operational criticality, long-term institutionalization, dependency on tacit knowledge, fragile technical implementation, and complex stakeholder negotiations around rationalization.

3.2.3 Participants and Access

The researcher was embedded as a functional analyst, collaborating with Appian developers, RPA specialists, Project managers, and IT architects. The role combined analytical responsibilities (AS-IS process analysis, requirement gathering), design activities (TO-BE process modeling in BPMN, Appian interface specification, RPA logic definition), and coordination functions (workshop facilitation, stakeholder alignment).

Through conversations with the bank and consulting team, empirical access evolved using a snowball sampling approach where new respondents emerged over time from various recommendations (Bryman, 2012). This selection process resulted in contact with six stakeholders with key roles and vast insight into the processes and rationalization initiatives.
Table 1 presents the sample overview, with participants given coded designations to ensure anonymity and to facilitate the reader's ability to identify statements in relation to organizational perspective.

Table 1 – Sample overview

Participant	Profile	Interview duration	Interview setting
OPS	Operations analyst for succession and sub-certification processes. Familiar with Access databases and reconciliation routines. 4 years of experience in back-office operations. (Bank employee)	20 min	Video call
BUS	Business tribe representative from Savings & Investment unit. Product expert responsible for submitting accounting letters and validating commission calculations. (Bank employee)	15 min	Video call
DEV	Developer from the consulting team, responsible for Appian platform governance, RPA implementations, bot development and maintenance.	35 min	In person
IT	IT architect responsible for integration with CAD and core banking systems. Overseeing process integrity and regulatory reporting. Authority over approval of rationalization initiatives and budget allocation. (Bank employee)	15 min	Video call
PM	Project manager from the consulting team, coordinating overall shadow IT rationalization initiative. Interface between bank stakeholders and technical delivery.	25 min	In person
AN	Senior functional analyst from the consulting team. Extensive experience in process reengineering and low-code platform design in financial services.	40 min	Video call

Participants' designated codes are based on their organizational role: operations (OPS), business tribes (BUS), IT and architecture (IT), Developer (DEV), project management (PM), and analyst (AN).

In addition to formal interviews, more than ten process-mapping and design workshops were organized, each typically involving three to six participants from different functions and lasting between 60 and 90 minutes. The researcher also had continuous access to project documentation, operational artifacts (macro-enabled spreadsheets, Access database schemas, workflow scripts), and informal interactions during daily project activities.

3.3 Data Collection: Intervention and Joint Sensemaking

Data collection combined semi-structured interviews, process-mapping workshops, focused analyses of shadow IT assets, and project documentation. These activities functioned simultaneously as data-gathering instruments and as organizational interventions that elicit hidden dependencies, inconsistencies, and tensions (Bryman, 2012; Dubois & Gadde, 2002; Staron, 2025).

To answer the research questions, semi-structured interviews were selected as the primary technique to create an in-depth understanding of shadow IT persistence, modernization challenges, and rationalization dynamics. Semi-structured interviews are appropriate for creating a broader understanding of a specific case and facilitating empirical data collection from practical experiences (Kvale & Brinkmann, 2015). Interviews enable an exchange of knowledge between interviewer and respondent in which questions can be adapted based on the person being interviewed to achieve the best possible result (Kvale & Brinkmann, 2015). The focus and follow-up questions were adjusted between interviews with operations, business, IT & Governance respondents to best capture both operational and strategic perspectives.

In order to ensure relevant knowledge regarding shadow IT persistence and rationalization processes, all respondents included in the study had key positions during the transformation initiative. Including only knowledgeable, key actors meant a restricted number of participating respondents. To counteract potential downsides of the smaller sample size, data collection also comprised reviewing project material, process design documents, and workshop outputs. Such a multi-method approach enables triangulation and increases reliability (Bryman, 2012). This approach enabled comparisons of respondents' answers with additional material, increasing reliability through triangulation and ability to cross-check the answers provided.

The empirical data collection followed the logic of the analytical framework based on the purpose, theoretical foundations, previous research, and research gaps presented in this study. The intention was to capture shadow IT persistence mechanisms, modernization outcomes, rationalization challenges, and organizational dynamics; in order to facilitate greater understanding of how shadow IT rationalization may be approached in banking digital transformation.
Table 2 presents the main themes of the interview guide and the logic behind their inclusion.

Table 2 – Interview themes

Theme	Objective
A - Interviewee profile and role	To understand the background and experience of the interviewee, contextualizing the collected data and ensuring relevance of participation in shadow IT processes or rationalization initiatives
B - Current shadow IT usage and AS-IS processes	To capture how shadow IT is actually used in daily operations, what functions it performs, dependencies with core systems, and why formal alternatives are insufficient (addressing RQ1 on persistence mechanisms)
C - Issues and challenges with shadow IT	To capture continuity risks, governance gaps, knowledge embeddedness, and operational fragility that motivate rationalization efforts and reveal lock-in dynamics
D - Modernization technologies: Appian, RPA, and workflow automation	To capture stakeholder perceptions of low-code and RPA as solutions or as new sources of risk, how these technologies are framed in governance discussions, and observed shifts in risk location (addressing RQ2 on modernization outcomes)
E - Rationalization dynamics and organizational factors	To capture negotiations over scope, ownership, approval authority, cost allocation, and collaboration patterns between business, IT, and governance functions that shape rationalization success or failure (addressing RQ3 on organizational dynamics)

The full interview guide was structured to enable comparison across different shadow IT domains while allowing flexibility to explore domain-specific issues.
The full interview guide can be found in **Table 3 – Interview guide.**

Process-mapping workshops played a particularly central role. In the GESPRO product census workshop, stakeholders initially described the process as "feeding CAD with the right product data." When the group mapped each step, it emerged that multiple validation routines—such as enforcing date rules, checking ID codes for formatting errors, verifying currency codes, managing decimal precision, and handling exceptions—were executed within the shadow IT application rather than in any governed platform. The realization that these controls were embedded in a local tool generated both surprise and discomfort: some participants downplayed its centrality, while others expressed concern about dependency on a single operator and system fragility.

In succession workshops focused on dossier closure, a critical process gap became evident when the historical Access database was discontinued following partial Appian migration: no formal mechanism remained to trigger timely closure of title dossiers after estate settlement,

leading to ad-hoc closures that sometimes occurred prematurely and required manual reopening. The workshop revealed conflicting interpretations of who should perform closures, how four-eyes checks should be documented, and whether existing RPA implementations replicated or corrected discontinued tool logic.

Workshops comparing stakeholder views—where business, operations, and governance representatives jointly reviewed draft process maps—served as arenas where conflicting interpretations were confronted. Debates about automation scope, approval authority, or bot behavior in ambiguous scenarios revealed misalignments central to understanding rationalization as negotiation. Process maps operated not merely as documentation, but as analytical and sensemaking tools that mediated organizational dialogue (Staron, 2025; Dubois & Gadde, 2002).

Formal project artifacts were collected throughout the engagement, including requirement documents, Appian process design documents, RPA specifications, system integration analysis, status reports, and stakeholder correspondence. Informal conversations and observations during day-to-day work were recorded in working notes and later used to enrich and cross-check interpretations. Combining multiple sources follows abductive case research recommendations to use triangulation not only for verification but also for discovery and redirection of analytical focus (Dubois & Gadde, 2002; Bryman, 2012).

Table 3 – Interview guide

Section	Main purpose	Core questions
Pre-interview	Clarify scope and ethics	Explain focus on shadow IT persistence, Appian/RPA modernization, and rationalization in the bank; define domains (GESPRO, succession, sub-certification, Server Platform); confirm anonymity, voluntary participation, and permission to take notes.
1. Profile and role	Contextualize answers	1) What is your current role and main responsibilities in the bank? 2) What experience do you have with the processes we discuss and with shadow IT/Appian/RPA? 3) What was your role in the shadow IT rationalization initiative, and for how long were you involved?
2. Shadow IT persistence (RQ1)	Understand why shadow IT persists and how	1) Which shadow IT tools (e.g., Excel macros, Access DBs, local spreadsheets) are critical in your process, and what do they do that formal systems cannot? 2) How are these tools connected to official systems (CAD or others)

	knowledge is embedded	and who maintains them? What happens if that person is unavailable? 3) Where is their logic documented? Why do you think these tools have remained in use for so long, and have there been attempts to replace them?
3. Modernization with Appian/RPA (RQ2)	Capture risk translation and governance effects	1) Which parts of your process were targeted for migration to Appian or RPA, and what benefits were expected? 2) How did you and other stakeholders perceive these technologies: mainly as risk-reducing solutions or also as sources of new risks (e.g., opacity, rigidity, new dependencies)? 3) In practice, did Appian/RPA reduce the risks linked to shadow IT or shift them elsewhere (for example to platform/vendor dependency or governance complexity)?
4. Organizational dynamics (RQ3)	Understand ownership, negotiation, and business–IT relations	1) Who "owns" the end-to-end process supported by these shadow IT tools? Is ownership clear or fragmented across units? 2) Were there conflicts or negotiations between business, operations, IT, and governance about priorities, design choices, or cost allocation in the rationalization? 3) What helped or hindered progress (e.g., sponsorship, process mapping workshops, alignment or mistrust between business and IT)?
5. Challenges, success factors, closing	Synthesize key lessons	1) What were the main challenges in trying to rationalize these shadow IT solutions, and how were they addressed? 2) What do you see as the main success factors for shadow IT rationalization in this bank? 3) Did this initiative change your view of shadow IT or modernization technologies? 4) Is there anything important about shadow IT persistence, modernization risks, or organizational dynamics that we have not discussed?

3.4 Analytical Strategy and Link to Research Questions and Gaps

The analytical strategy followed an abductive, mechanism-oriented logic. Empirical material from field notes, workshop summaries, interview transcripts, and project documents was repeatedly read to identify recurring patterns—such as dependence on particular spreadsheets, disputes over process scope, or narratives about bots "taking over" manual work. These incidents were clustered into provisional categories and iteratively refined through engagement with relevant literature (Dubois & Gadde, 2002; Bryman, 2012). Emerging interpretations were systematically checked against multiple data sources to avoid over-reliance on single episodes (Dubois & Gadde, 2002; Guest et al., 2011).

The analysis was explicitly structured to address the three research questions and research gaps identified in Chapter 2. For **RQ1** (mechanisms of shadow IT persistence), attention was directed to routinization in everyday work, accumulation of dependencies between shadow assets and core systems, and embedding of critical knowledge in local tools rather than formal documentation. This addresses **Research Gap 1** on insufficient theorization of shadow IT as a long-term, path-dependent phenomenon. Observations from GESPRO, succession, sub-certification, and reconciliation processes revealed that shadow IT evolves from workaround to de facto infrastructure, functioning as institutional memory that survives individual staff changes. The analytical categories "operational dependency and embedded logic" and "shadow IT as institutional memory" emerged from iterative engagement with these patterns.

For **RQ2** (governance outcomes of modernization technologies), the analysis examined episodes where stakeholders framed low-code, RPA, or workflow automation as either amplifying or mitigating risk. This addresses **Research Gap 2** on ambiguous governance outcomes of modernization and conditions under which these technologies reproduce or relocate risks. The analysis examined how technologies reconfigured risk: in some areas improving input standardization and traceability; in others translating logic into more opaque or rigid technological layers and shifting risk from technical failure to governance and comprehension challenges. Episodes where stakeholders framed modernization as enabling control versus creating new dependencies were analyzed as moments where competing interests sought to reshape governance arrangements, echoing prior findings that risk is a central power-shifting construct in attempts to control shadow systems in banks. The analytical category "modernization as risk translation" captures this finding.

For **RQ3** (organizational dynamics and rationalization effectiveness), focus was on fragmented process ownership, negotiations over boundaries and scope, contests over who funds and benefits from automation, and mismatches between formal governance structures and operational realities. This addresses **Research Gap 3** on how organizational factors—silos, weak collaboration, ambiguous ownership—undermine rationalization efforts. The analysis examined instances where modernization initiatives stalled not due to technical barriers but due to unresolved questions about rule ownership, accountability for exceptions, and cost allocation across units. The analytical categories "fragmented ownership and structural limits to rationalization" and "rationalization as organizational

negotiation" emerged from systematic comparison of cases where rationalization progressed versus cases where it stalled or resulted in hybrid solutions.

When reconstructing these trajectories, particular attention was given to instances where informal tools were not eliminated but re-anchored at the business level with partial governance by IT, consistent with emerging distinctions between shadow IT, business-managed IT, and IT-managed systems. This perspective allowed differentiation between shadow IT that remains in the margins and shadow arrangements progressively domesticated and integrated into formal governance.

By orienting the analysis toward mechanisms rather than isolated observations, the thesis aims to refine and extend current understandings of shadow IT persistence and governance, in line with identified research gaps. The mechanisms identified—operational dependency and embedded logic, shadow IT as institutional memory, modernization as risk translation, and rationalization as negotiation under fragmented ownership—are systematically developed in Chapter 4 and explicitly connected back to the three research questions and gaps that structure the thesis.

3.5 Quality, Limitations, and Ethical Considerations

Quality is assessed in terms of credibility, dependability, and transparency (Bryman, 2012; Yin, 2009). Credibility was enhanced through data triangulation across interviews, workshops, documents, and informal observations; methodological triangulation combining action research, semi-structured interviews, and process mapping; and analytical triangulation via iterative discussion with academic supervisors (Bryman, 2012; Dubois & Gadde, 2002). Dependability was supported by maintaining an audit trail of key analytical decisions, including memos documenting how initial themes were refined into the mechanisms presented in Chapter 4 (Dubois & Gadde, 2002).

The design entails limitations. The researcher did not control project scope or pacing, which constrained the ability to systematically plan data collection around all relevant events. Access was concentrated in four domains, so some aspects of the bank's broader shadow IT landscape remain outside the empirical scope. The hybrid consultant-researcher role may have influenced how stakeholders presented problems, potentially reinforcing certain framings over others. However, in line with action research guidelines, these limitations are inseparable from the advantages of deep, situated access, which enabled observation of fine-grained dynamics difficult to capture through detached methods (Staron, 2025; Bleijenbergh et al., 2020).

Ethically, the bank is not named and individual stakeholders are anonymized; process descriptions avoid disclosing sensitive commercial or security-relevant details. Data were collected as part of ordinary project activities, and their academic use is limited to high-level analysis of organizational patterns and mechanisms. The study follows general ethical principles for organizational and action research, including transparency with key stakeholders, avoidance of harm, and careful handling of internal documents (Bryman, 2012; Staron, 2025).

4. Empirical Findings

4.1 Structure

In this chapter, the findings of the qualitative data collection and the action research intervention will be presented. The analysis is structured into clusters of themes that emerged during the internship, rigorously following the analytical model developed in Chapter 3. These themes directly address the three research questions regarding the persistence of Shadow IT, the implications of modernization through low-code/RPA, and the organizational dynamics of rationalization.

First, a comprehensive contextual analysis of the case study and the strategic reasoning behind the rationalization project will be presented to ground the subsequent findings (Section 4.2). The empirical evidence is then deconstructed according to the specific research gaps:

- **Section 4.3** addresses **RQ1** (*Persistence*), dissecting the mechanisms of operational dependency and institutional memory that render shadow tools indispensable.
- **Section 4.4** addresses **RQ2** (*Modernization*), critically examining how the transition to Appian and RPA reconfigures risk profiles rather than simply eliminating them.
- **Section 4.5** addresses **RQ3** (*Organizational Dynamics*), exploring the friction caused by fragmented ownership and the political nature of rationalization.
- **Section 4.6** provides a synthesis of the identified mechanisms.

Throughout the text, empirical data from participant observations, document analysis (specifically the "AS-IS" process mappings), and semi-structured interviews are integrated into the narrative. References to respondents are made using the abbreviations established in the methodology (e.g., **OPS** for Operations Analyst, **BUS** for Business Tribe, **IT** for IT Architect, **PM** for Project Manager, **DEV** for Lead Developer, **AN** for Senior Functional Analyst).

4.2 Contextual Foundation: The Strategic Imperative and Operational Reality

To fully grasp the mechanisms at play, it is essential to first reconstruct the operational reality of the "Financial Services Transformation" project. The empirical setting was a major Italian banking institution where the internship was conducted within the consulting team responsible for the "decommissioning" of critical Shadow IT assets.

4.2.1 The Case Organization and Project Scope

The bank’s strategic initiative was not merely a technical upgrade but a governance intervention. The management had identified a systemic risk: core operational processes were

running on "User-Developed Applications" (UDAs)—primarily complex Excel macros and Access databases—that operated outside the formal control of the IT department. The project aimed to replace these assets with a "Sanctioned IT" architecture composed of **Appian** (a low-code platform for process orchestration and data entry) and **RPA** (Robotic Process Automation for legacy system interaction).

As respondent **PM** explained during the initial strategic alignment, the project was framed to stakeholders not as a restriction of their freedom, but as a "risk translation" exercise. The PM emphasized that for the business, the selling point was "traceability—no more lost emails," while for IT, the value proposition was "compliance." This dual framing was necessary because, as the empirical observation revealed, the shadow tools were effectively "free" for the departments using them, whereas the modernization required significant capital investment. The persistence of these tools was, therefore, initially driven by a distorted economic incentive where hidden operational costs were ignored in favor of zero license costs.

4.2.2 The Archaeology of the "AS-IS": Mapping the Shadow Landscape

The "AS-IS" analysis phase of the internship revealed that the targeted processes were characterized by a high degree of fragmentation and reliance on "tribal knowledge." The investigation focused on four primary clusters, each representing a different archetype of Shadow IT:

1. **GESPRO (Revenue Management):** This process governed the monthly management of millions of euros in commissions owed to asset managers. It relied on a "Shadow IT" asset—a dense layer of Excel workbooks and VBA macros that orchestrated data between external "tribes" and the legacy CAD accounting system.
2. **Successions (The Diary):** A workflow for managing inheritance dossiers, which relied on a legacy Access database. This tool, known internally as "The Diary," functioned as the single source of truth for the status of thousands of sensitive files, bridging the gap between the rigid host system and the fluid reality of legal documentation.
3. **Sub-certification:** A regulatory reporting process involving the reconciliation of data across heterogeneous sources (NEXIM, CAD, Neolink). It was orchestrated entirely through local macros that performed complex "vlookups" and data cleaning operations that no formal system supported.
4. **Platform Server:** A contract management tool developed internally by a single employee to manage billing cycles and FTE reporting for intragroup services. It lacked formal documentation, yet it governed the invoicing of service levels across the banking group.

The findings presented below draw directly from the "deep dive" workshops conducted to reverse-engineer these tools.

4.3 RQ1: The Mechanics of Persistence

The first set of findings answers **RQ1**: *What organizational mechanisms contribute to the long-term persistence of Shadow IT in banking institutions?*
The empirical data challenges the simplistic view of Shadow IT as a mere "workaround" for slow IT delivery. Instead, the analysis suggests that these tools persist because they evolve into indispensable infrastructural layers—a phenomenon identified here as Operational Dependency—and because they serve as the primary repository of Institutional Memory.

4.3.1 Operational Dependency: The Shadow Tool as "Middleware"

The most significant finding regarding persistence is that shadow tools effectively function as an unacknowledged "middleware" layer. They do not just store data;
they contain the *connective logic* that allows incompatible systems to talk to one another.

This was most vividly illustrated in the **GESPRO** process. The official procedure described a linear flow: receive commission data, check it, and upload it to the CAD system. However, the analysis of the "JUG2" and "JUG5" macros revealed a radically different reality. These macros were not simple data loaders; they were complex integration engines interacting with the mainframe via "Reflection" terminal emulation. As respondent **AN** (Senior Analyst) observed during the mapping phase, the biggest surprise was the "discrepancy between the Process on Paper and the Process in Excel." While the formal procedure simply stated "Check data," the macro contained thousands of lines of code executing specific business rules: "if the currency is USD, truncate to 2 decimals; if the client is VIP, ignore the error."

This embedded logic creates a form of "lock-in." The organization cannot simply remove the Excel file because it no longer understands the rules contained within it. For instance, during the "Censimento" analysis, it was discovered that the shadow tool automatically handled specific exceptions for "Assicurativi" (Insurance products) versus "Gestito" (Managed products). It applied different variance thresholds—permitting autonomous postings when deviations were below 5 euros—without the operator needing to intervene.
Respondent **BUS** (Business Tribe Rep) staunchly defended this setup, arguing that the persistence of these tools was a rational response to market velocity. He noted that commission structures changed every six months with new product launches, whereas the bank's IT release cycles were far slower. For him, the tool was not "shadow" but "agile," essentially a mechanism to decouple business speed from IT latency.

Consequently, the shadow tool persists because it absorbs the complexity that the formal system (CAD) cannot handle. It validates ISIN codes to ensure no spaces are present—a check that, if failed in the mainframe, would cause a system crash—and it normalizes date formats that vary across different external providers. Removing this layer without replicating its full complexity would effectively halt the process.

4.3.2 Institutional Memory and the "Frozen Policy"

The second mechanism driving persistence is the role of Shadow IT as a vessel for **Institutional Memory**. In an environment characterized by staff rotation and heavy reliance on external consultants (e.g., Accenture), the shadow tool often becomes the only artifact that "remembers" how the process actually works.

This phenomenon was most evident in the **Successions** process with the "Access Database" (The Diary). During interviews, respondent **OPS** (Operations Analyst) explained that the formal CAD system was purely accounting-based—it could record a transaction, but it could not tell the *story* of a dossier. The Access database tracked whether a file was waiting for documents, ready for closure, or suspended due to a missing notary signature. OPS emphasized that this tool survived because it was "the only place where the truth of the process lived." If the colleague who built it had not maintained it, the team would have been "lost in emails."

The shadow tool acts as a "frozen policy," capturing decisions made years ago that have never been formally documented. In the **Sub-certification** process, the analysis of the "Title Reconciliation" macros (specifically for handling 10.331 and 10.131 file formats) revealed hard-coded lists of "known exceptions." These were ISIN codes or transaction types that had caused errors in the past and were now automatically filtered out by the macro. Current operators used the tool daily but could often not explain *why* a certain code was excluded; they simply knew that "the macro handles it."

This creates a paradox where the organization is afraid to modernize because it fears losing this accumulated wisdom. As respondent **DEV** (Lead Developer) noted, the logic persisted in the code because "nobody dared to touch it." The Shadow IT asset had become a load-bearing structure held together by "duct tape," containing validation rules—such as checking for specific ISIN formats—that existed nowhere else in the bank's documentation. To retire the tool was to risk inducing amnesia in the process itself.

4.4 RQ2: Modernization and the Translation of Risk

The second set of findings addresses **RQ2**: *To what extent do low-code platforms and RPA mitigate shadow IT-related risks, and under what conditions do they generate new forms of opacity or dependency?*

The empirical data supports the hypothesis of "Risk Translation." While the project succeeded in mitigating specific *technical* risks (e.g., data loss, lack of backups, single-person dependency), it systematically introduced new *governance* and *operational* risks. The transition from Excel/Access to Appian/RPA was not a zero-sum game of risk reduction but a complex reconfiguration of where the risk resided.

4.4.1 From Operational Flexibility to Algorithmic Rigidity

A recurring theme in the findings was the tension between the chaotic flexibility of Shadow IT and the structured rigidity of the sanctioned solution. The shadow tools allowed for "local adjustments" that, while formally non-compliant, were operationally essential for keeping the business moving.

In the analysis of the **Platform Server** replacement, this tension was palpable. The shadow tool allowed the user to manage billing for "creative" contractual arrangements—such as bundling services, applying ad-hoc commercial discounts, or managing "VAT exemption" status through manual flags. The proposed Appian solution, by contrast, required a strict cataloging of services and rigorous adherence to standard billing models.
Respondent **BUS** expressed deep concern about this shift, noting that while IT viewed the Excel file as a "risk to be killed," he viewed it as a "calculator" that allowed him to do his job. He warned that the new system introduced "rigidity risk": if he had a commercial exception, he could previously just adjust the Excel cell; now, Appian would reject the input if it didn't match the standard logic, requiring him to open a ticket and wait.

This finding suggests that modernization often strips away the "shock absorbers" that Shadow IT provides. Respondent **BUS** succinctly summarized this trade-off: "The risk of error is lower, but the risk of business paralysis is higher." The "Appian" solution enforced a "Happy Path" that accounted for 80% of standard cases but struggled with the 20% of exceptions that the shadow tool handled effortlessly through manual intervention. This was further complicated by the "VAT exemption" issue, where the shadow tool allowed for manual handling of tax statuses that the formal SAP integration was not yet ready to support, forcing the project team to build temporary workarounds within the "modern" solution—effectively recreating a shadow process within the formal tool.

4.4.2 The "Black Box" Paradox: Visibility vs. Intelligibility

The introduction of RPA (Robotic Process Automation) to replace VBA macros created a "Black Box" effect. While the new system offered superior *traceability* (logs, dashboards), it offered inferior *intelligibility* to the actual operators.

In the **GESPRO** automation, the VBA macros were legible to the advanced business users; if a calculation looked wrong, they could open the code, trace the formula, and understand the logic. With the move to RPA, the logic was encapsulated in a bot running on a remote server. As respondent **OPS** described, the feeling was mixed: "Appian is cleaner... But we lost flexibility." The operators felt they had traded a tool they understood for a "black box" they couldn't control. This was not just a feeling but an operational reality.
The **Successions** decommissioning revealed a critical "process gap": the old Access database had a built-in trigger that alerted operators to close a dossier 10 days after a specific event. The new Appian workflow handled the document flow but initially missed this temporal trigger because the developers had focused on the "action" rather than the "waiting period." This led to premature closures by the bot, a failure that respondent **OPS** attributed to the system "following a rigid rule that didn't account for the reality."

Respondent **DEV** confirmed this translation of risk from a technical perspective. He described RPA as a "band-aid" that often "cemented the bad process." By replicating the macro's keystrokes with a bot, the project shifted the risk from "execution errors" (fat-finger mistakes) to "maintenance risks." If the legacy CAD system changed a screen pixel or a field layout, the macro might have failed, but the user could have fixed it or worked around it. The bot, however, would simply break, requiring a specialized developer to intervene. Thus, dependency shifted from the "macro-guru" in the business unit to the "RPA developer" in the IT unit, without necessarily reducing the overall fragility of the ecosystem. Respondent **IT** (IT Architect) reinforced this view, characterizing RPA as "Server-side Shadow IT"—a compromise that traded the unknown risk of Excel on a desktop for the managed, yet fragile, risk of bots in a data center.

4.5 RQ3: Organizational Dynamics and the Politics of Rationalization

The third set of findings addresses **RQ3**: *How do organizational dynamics, stakeholder alignment, and end-to-end process ownership shape the effectiveness of shadow IT rationalization?*
The internship observations revealed that "rationalization" is less of a technical challenge and more of a political negotiation regarding ownership, boundaries, and power. The technical act of replacing software served as a catalyst that exposed latent organizational conflicts.

4.5.1 Fragmented Ownership and the "No-Man's Land" of Process

A major impediment to the project was the lack of clear end-to-end ownership, a phenomenon best described as "Fragmented Ownership." Shadow IT had thrived precisely because it filled the gaps between organizational silos. When the project team attempted to remove the shadow tools, these gaps became visible and problematic.

In the **Successions** domain, the process was structurally fragmented. The input came from the branch network, the processing was done by Operations, and the final closure was often dependent on external vendors (Wave 1, Wave 2) or third-party providers (Accenture). The "Internship Reflection" notes documented a specific crisis regarding the **closure of dossier titles**. The analysis revealed that the closure was executed in a non-coordinated way: the external provider executed a closure via their own macro-robot, while the internal team manually fixed the unmatched residues. No single entity owned the entire lifecycle.

Respondent **PM** highlighted that this fragmentation was the biggest hurdle. "When we mapped the process, everyone pointed fingers," he noted. The "Access Database" had acted as the glue holding these fragmented parts together; without it, the stakeholders were forced to confront the fact that they didn't agree on the process definition. Questions arose: Who is responsible for the "spunta" (validation) step in the new digital flow? Who owns the "business rule" for exception handling? Respondent **IT** emphasized the difficulty of these negotiations, noting that he had to be the "bad cop" to refuse Superuser access to the bots, forcing the Business to accept that they—not IT—owned the data quality.

4.5.2 Rationalization as a Negotiation of Power and Meaning

The most effective mechanism for overcoming this fragmentation and achieving rationalization was found to be "Collaborative Visualization"—specifically, the creation of what the team called the "Wall of Truth."

During the **GESPRO** analysis, the internship task involved printing large, wall-sized BPMN diagrams that visualized the hidden complexity of the macros. This physical artifact became a boundary object that facilitated negotiation. As respondent **AN** described, the "Wall of Truth" was the turning point: "The Business saw the complexity and said, 'We do all that?' It made the Shadow visible. It stopped being a technical update and became an organizational cleanup."

This finding indicates that technical rationalization requires a prerequisite phase of "social rationalization." In the **Sub-certification** meetings, different teams (Accounting vs. Operations) discovered they were using the same terms—such as "reconciliation" or "closure"—to mean completely different activities. The shadow tools had allowed them to maintain these divergent definitions in isolation, as each team had its own private Excel file. The modernization project forced a semantic negotiation.

Successful rationalization occurred only when the project team moved beyond "requirements gathering" to "negotiation facilitation." For instance, in the **Title Reconciliation** workflow, the conflict between the Business (who wanted flexibility) and IT (who wanted security) was resolved not by one side winning, but by a "Human-in-the-loop" design compromise. As respondent **DEV** explained, success came when they stopped trying to automate 100% of the process. They automated the 80% standard cases and routed the 20% "weird ones" to Appian for human review. This saved the project because it acknowledged the political reality that the Business needed to retain control over exceptions.

Furthermore, the "Platform Server" analysis revealed conflicts over **Cost Allocation**. The functions expected to fund the Appian licenses were not necessarily the ones reaping the operational savings, creating resistance. The project succeeded only when the PM framed the initiative as "Risk Translation"—selling compliance to IT and traceability to Business—thereby aligning the divergent interests of the stakeholders.

4.6 Synthesis of Empirical Findings

The empirical findings presented in this chapter reveal a complex interplay between technology, agency, and organizational structure. The persistence of Shadow IT in the banking sector is not an anomaly but a structural adaptation.

1. **Persistence is Structural:** Shadow IT persists due to **Operational Dependency**—the tool performs critical "middleware" functions that the rigid legacy core cannot—and **Institutional Memory**, where the tool acts as a repository of historical context and "frozen policy" that the organization has otherwise forgotten.

2. **Modernization is a Trade-off:** The transition to Low-Code and RPA is not a linear upgrade but a process of **Risk Translation**. The organization trades the *operational risk* of manual errors and data loss for the *structural risk* of algorithmic rigidity and "black box" opacity. The new systems are more robust but less intelligible to the users who depend on them.
3. **Rationalization is Political:** The success of decommissioning efforts is contingent on resolving **Fragmented Ownership**. Shadow IT often exists to bridge the "no-man's land" between organizational silos. Removing it requires not just new software, but a renegotiation of roles, responsibilities, and definitions—a process where "social rationalization" via collaborative mapping is as critical as the technical implementation itself.

These findings suggest that the "problem" of Shadow IT is actually a symptom of a deeper disconnect between the bank's static formal governance and its dynamic operational reality. The "solution," therefore, lies in the realignment of these organizational plates, with technology serving merely as the medium for this new social contract.

5. Discussion

This chapter synthesizes the empirical findings with the theoretical foundations established in the Literature Review, addressing the three research questions that guided this investigation. The analysis reveals how Shadow IT rationalization in banking represents not merely a technical modernization challenge, but a complex socio-technical transformation involving path dependencies, risk reconfiguration, and organizational negotiation. The discussion is structured around the three research questions before articulating broader theoretical contributions, managerial implications, and concluding reflections.

5.1 Shadow IT Persistence: Confirming and Extending Theory

The first research question examined the organizational mechanisms contributing to long-term Shadow IT persistence in banking institutions. The empirical findings strongly confirm and extend existing theoretical frameworks while revealing mechanisms insufficiently addressed in prior literature.

Operational Dependency as Middleware Lock-In

The literature identified routinization, knowledge embeddedness, substitution failure, and organizational dependency as key persistence drivers (Fürstenau et al., 2017; Rakovic, 2020), yet these concepts remained largely descriptive rather than explanatory. This study extends the concept of operational dependency by demonstrating that Shadow IT tools function as unacknowledged middleware layers performing critical integration and validation functions between rigid legacy systems and dynamic business requirements. The GESPRO case revealed that Excel macros executed thousands of lines of business logic—currency truncation rules, ISIN validation protocols, variance thresholds—that existed nowhere in formal system documentation. This aligns with Fürstenau et al.'s (2017) observation that shadow systems in banking often support core rather than peripheral processes, but extends it by demonstrating precisely *how* such criticality emerges through the gradual accumulation of connective logic bridging architectural gaps left by legacy systems.

The concept of technical debt (Khabouze, 2022; Monaghan et al., 2020) provides a complementary lens. This study reveals why modernization strategies encounter resistance: shadow tools have become load-bearing structures whose removal threatens operational continuity. Organizations cannot simply replace these tools without first comprehensively understanding and replicating their embedded logic—a requirement that contradicts the *raison d'être* of Shadow IT, which thrives precisely because its logic remains undocumented and tacit.

Institutional Memory and Frozen Policy

The second persistence mechanism—Shadow IT as institutional memory—confirms Rakovic's (2020) observation that informal systems evolve from gap-filling to replacement roles when formal systems fail to adapt. This study contributes a temporal dimension: shadow

tools become vessels for *frozen policy*, capturing historical decisions and business rules that current operators can execute but cannot explain. The Successions Access database exemplified this, functioning as the sole repository of dossier status information that the formal CAD system could not accommodate.

This reveals a more insidious dynamic than Behrens' (2009) "hit-by-a-bus" scenario: even when knowledgeable individuals remain present, the rationale embedded in shadow tools becomes opaque over time as business contexts evolve while tools remain static. Organizations develop *technological amnesia*—an inability to reconstruct the reasoning behind automated decision-making. This challenges the literature's implicit assumption that persistence primarily reflects ongoing satisfaction with shadow solutions (Klotz et al., 2019). Instead, persistence often reflects *fear of loss*—organizations continue using shadow tools not because they work well, but because no one fully understands what would break if they were removed.

Theoretical Contribution

The empirical findings substantiate the theoretical distinction between adoption drivers and continuation drivers (Klotz et al., 2019; Fürstenau et al., 2017; Rakovic, 2020), demonstrating that tools initially created due to IT unresponsiveness persist due to fundamentally different mechanisms involving technical debt, fragmented architectures, knowledge distribution, and power dynamics. This requires analytical frameworks grounded in path dependency theory and institutional theory (Berente et al., 2008; Azad & King, 2012) rather than technology acceptance models.

5.2 Modernization as Risk Translation: Challenging Technological Optimism

The second research question interrogated the extent to which low-code platforms and RPA mitigate shadow IT-related risks versus generating new forms of opacity or dependency. The findings fundamentally challenge the technological optimism pervading practitioner discourse while confirming emerging academic skepticism.

From Flexibility to Rigidity

The empirical evidence reveals a paradox: while platforms like Appian and RPA demonstrably improve certain risk dimensions—audit trails, standardized workflows, backup procedures—they simultaneously introduce structural rigidities that shadow tools had masked. This aligns with Shah's (2025) quantitative findings that governance maturity predicts compliance error reduction but not cost savings. The Platform Server case illustrated this tension: the shadow tool permitted ad-hoc commercial arrangements and manual VAT handling, providing operational flexibility that the proposed Appian solution explicitly disallowed. Respondent BUS characterized this as trading "error risk" for "business paralysis risk"—a formulation capturing the fundamental trade-off between control and adaptability.

This supports Shah's (2025) conclusion that these platforms shift where and how shadow-IT-like risks manifest rather than eliminating them. Opacity moves from undocumented Excel macros to proprietary platform configurations; dependency shifts from local "macro-gurus" to specialized RPA developers; knowledge gaps transition from business-side tribal expertise to IT-side technical specialization. The study thus extends Spivey and McIlveene's (2024) governance framework by demonstrating empirically that prohibition-based approaches fail because they misconceive the problem: shadow solutions persist because they absorb complexity that formal systems cannot accommodate.

The Black Box Paradox

A second key finding concerns the *black box paradox*: modernization platforms provide superior *visibility* (audit logs, dashboards, process analytics) while simultaneously reducing *intelligibility* for operational staff. This contradicts the assumption that technical transparency automatically enhances substantive governance (Panko, 2006; Zimmermann et al., 2017). The GESPRO case revealed that business users could interrogate VBA macro logic when results appeared incorrect, enabling local troubleshooting. RPA implementations, by contrast, encapsulated this logic in server-side bots opaque to end-users, creating new dependencies on specialized technical staff.

This finding has significant implications for compliance in regulated banking environments. While regulatory frameworks including GDPR, Basel III, and DORA demand transparency and traceability (Spivey & McIlveene, 2024), the study reveals that *formal* compliance—documented processes, audit trails, access controls—does not guarantee *substantive* control when underlying logic remains opaque to those responsible for operational outcomes.

Theoretical Contribution

The study's central theoretical contribution regarding modernization lies in reconceptualizing it as *risk reconfiguration* rather than risk reduction. Where prior literature focused on efficiency gains and compliance benefits (Shah, 2025), this research demonstrates that automation platforms introduce qualitatively different risk profiles involving algorithmic rigidity, black box intelligibility deficits, and governance capability dependencies. The conditions under which modernization genuinely reduces governance risk appear narrow: implementation requires not merely technical integration but also organizational restructuring to ensure governance structures possess the interpretive capacity to scrutinize platform-mediated processes.

5.3 Organizational Dynamics and Rationalization Effectiveness

The third research question explored how organizational dynamics, stakeholder alignment, and process ownership shape rationalization effectiveness. The findings decisively confirm that rationalization is fundamentally an organizational-political challenge rather than a technical-integration problem.

Fragmented Ownership as Structural Impediment

The empirical evidence strongly supports prior research identifying fragmented process ownership as a critical barrier to rationalization (Fürstenau et al., 2017; Nugraha et al., 2025; Zimmermann et al., 2017). The Successions case exemplified this: inputs originated from branch networks, processing occurred in Operations, and closures depended on external vendors, yet no single entity owned end-to-end accountability. The Access database functioned as organizational glue across these fragmented responsibilities, and its removal exposed latent conflicts regarding accountability, exception handling authority, and data quality ownership. This confirms Fürstenau et al.'s (2017) finding that decommissioning efforts fail when underlying causes—structural distance, weak trust, ambiguous ownership—remain unaddressed, but extends it by demonstrating that shadow tools actively *mask* such fragmentation, allowing organizations to defer resolving coordination problems until forced by modernization initiatives.

Rationalization as Negotiation

A particularly significant empirical contribution concerns the role of *collaborative visualization* as a rationalization enabler. The "Wall of Truth"—large-format BPMN diagrams mapping hidden macro complexity—functioned as a boundary object that made implicit assumptions explicit and facilitated stakeholder negotiation. This finding extends research on cross-functional collaboration (Fagbore et al., 2024) by demonstrating that effective rationalization requires not merely hybrid teams but also specific artifacts and practices that enable *semantic negotiation*. The Sub-certification case revealed that different units used identical terminology—"reconciliation," "closure"—to describe fundamentally different activities, a divergence that shadow tools had allowed to persist in isolation.

This aligns with Spivey and McIlveene's (2024) emphasis on shadow IT governance committees and flexible IT policy frameworks, but specifies the *mechanisms* through which such governance operates effectively: by creating forums and artifacts that transform rationalization from a unilateral IT intervention into a collaborative organizational learning process.

Theoretical Contribution

The study's core theoretical contribution regarding organizational dynamics lies in demonstrating that *social rationalization* is a prerequisite for effective *technical rationalization*. Shadow IT rationalization cannot succeed through technology replacement alone; it requires prior or concurrent resolution of organizational ambiguities regarding process ownership, role definitions, accountability structures, and semantic alignment. This challenges IT governance literature that treats organizational factors as contextual variables rather than as primary determinants of intervention effectiveness.

5.4 Practical Implications for Banking Digital Transformation

The study generates several actionable implications for banking institutions pursuing Shadow IT rationalization through low-code, RPA, and digital process automation.

First, banks must recognize that shadow IT persistence reflects structural organizational conditions rather than user deviance or IT department failures. Effective governance requires diagnosing why formal systems cannot accommodate legitimate business needs and addressing those architectural and organizational gaps, rather than simply prohibiting unauthorized tools (Spivey & McIlveene, 2024). This may require legacy system modernization investments that improve flexibility alongside organizational restructuring to clarify process ownership and accountability (Khabouze, 2022).

Second, modernization initiatives should adopt realistic expectations regarding risk transformation. Low-code and RPA platforms do not eliminate shadow IT risks but reconfigure them, trading operational flexibility and local intelligibility for standardization and audit trails. Banks must explicitly evaluate whether this trade-off aligns with specific process characteristics—highly standardized, high-volume transactions may benefit substantially, while processes requiring frequent adaptation may experience reduced operational effectiveness (Shah, 2025).

Third, rationalization projects must prioritize organizational alignment and semantic negotiation alongside technical integration. Establishing cross-functional teams, creating boundary objects that facilitate stakeholder dialogue, and investing in collaborative process mapping can transform rationalization from a contested IT imposition into a joint organizational learning opportunity (Nugraha et al., 2025; Fagbore et al., 2024). Banks should institutionalize such practices through automation centers of excellence or similar structures.

Fourth, organizations should develop explicit strategies for managing institutional memory embedded in shadow tools, including systematic documentation of business rules prior to decommissioning, phased migration approaches allowing parallel operation and knowledge transfer, and investment in cross-training to distribute critical expertise more broadly (Khabouze, 2022).

6. Conclusion and Future Research

This thesis examined Shadow IT rationalization in banking through an action research intervention in a major Italian banking institution. By investigating how Excel macros, Access databases, and other informal tools were replaced with low-code platforms and RPA, the research addressed three interconnected questions regarding persistence mechanisms, modernization outcomes, and organizational dynamics. The findings reveal that Shadow IT rationalization is fundamentally a socio-technical challenge requiring coordinated transformation of technology, governance structures, and organizational relationships.

6.1 Summary of Contributions

The thesis makes three primary theoretical contributions. First, it refines the conceptualization of Shadow IT persistence by demonstrating that informal tools function as unacknowledged middleware layers and institutional memory repositories. While prior literature identified persistence drivers, this study specifies *how* shadow tools become operationally irreplaceable through gradual accumulation of connective logic bridging legacy system gaps and through embodiment of frozen policy that current operators execute but cannot explain. This extends path dependency theory by showing that persistence reflects organizational fear of knowledge loss rather than ongoing satisfaction with shadow solutions.

Second, the research reconceptualizes modernization as risk reconfiguration rather than risk reduction. The empirical evidence demonstrates that low-code platforms and RPA shift risks from execution errors and data loss to algorithmic rigidity and black box intelligibility deficits. This challenges technological optimism in practitioner discourse by revealing that formal compliance—audit trails, process documentation, access controls—does not guarantee substantive control when platform logic remains opaque to operational staff responsible for outcomes.

Third, the study establishes that social rationalization is a prerequisite for technical rationalization. Shadow IT thrives in organizational gaps created by fragmented process ownership, and its removal exposes latent conflicts regarding accountability, exception handling authority, and semantic definitions. Collaborative visualization through boundary objects such as process maps enables stakeholder negotiation that transforms rationalization from contested IT imposition into joint organizational learning.

Practically, the findings offer actionable guidance for banking digital transformation initiatives. Banks should diagnose structural conditions driving shadow IT adoption rather than prohibiting tools; adopt realistic expectations regarding risk trade-offs when selecting processes for automation; prioritize organizational alignment and semantic negotiation through cross-functional teams and facilitated dialogue; and develop explicit strategies for preserving institutional memory embedded in shadow tools through phased migration and knowledge transfer.

6.2 Limitations and Future Research

The study's limitations suggest productive avenues for future research. The single-case design, while enabling deep contextual analysis, limits generalizability across banking contexts. Comparative studies examining shadow IT rationalization in banks with different legacy architectures, regulatory environments, or governance maturity levels could reveal how contextual factors moderate the identified mechanisms.

The ex-post action research design meant the researcher did not control project scope or timing, constraining systematic data collection around all relevant events. Prospective longitudinal studies tracking rationalization initiatives from inception through post-implementation stabilization could illuminate how persistence mechanisms, risk profiles, and organizational dynamics evolve over extended timeframes.

The research focused on four operational domains; broader organizational-level investigations could examine how shadow IT rationalization interacts with enterprise-wide digital transformation programs, revealing interdependencies between local interventions and strategic governance reforms.

Future research should also investigate conditions under which modernization platforms genuinely reduce governance risk rather than relocating it, particularly examining the role of governance capability development, platform configurability, and organizational learning mechanisms. Finally, comparative analysis of different rationalization approaches—including hybrid models that deliberately maintain selective shadow IT under explicit governance arrangements—could refine understanding of when formalization versus managed informality represents optimal strategy.

References

Abildtrup, A. (2024) 'The rise of robotic process automation in the banking sector: Streamlining operations and improving efficiency', Journal of Computing and Natural Science, 4(1), pp. 27–33.

Azad, B. and King, N. (2012) 'Institutionalized computer workaround practices in a Mediterranean country: an examination of two organizations', European Journal of Information Systems, 21(4), pp. 358–372.

Behrens, S. (2009) 'Shadow systems: The good, the bad and the ugly', Communications of the ACM, 52(2), pp. 124–129.

Berente, N., Yoo, Y. and Lyytinen, K. (2008) 'Alignment or drift? Loose coupling over time in NASA's ERP implementation', in Proceedings of the 29th International Conference on Interaction Sciences.

Bleijenbergh, I., van Mierlo, J. and Bondarouk, T.V. (2020) 'Closing the gap between scholarly knowledge and practice: guidelines for HRM action research', Human Resource Management Review, 31, 100764.

Bryman, A. (2012) Social Research Methods. 4th edn. Oxford: Oxford University Press.

Dubois, A. and Gadde, L.-E. (2002) 'Systematic combining: An abductive approach to case research', Journal of Business Research, 55(7), pp. 553–560.

Fagbore, O., Ogeawuchi, J., Ilori, O., Isibor, N., Odetunde, A. and Adekunle, B. (2024) 'Building cross-functional collaboration models between compliance, risk, and business units in finance', International Journal of Scientific Research in Science and Technology, 11, pp. 488–524.

Fürstenau, D., Rothe, H. and Sandner, M. (2017) 'Shadow systems, risk, and shifting power relations in organizations', Communications of the Association for Information Systems, 41(3), pp. 43–61.

Guest, G., MacQueen, K.M. and Namey, E.E. (2011) Applied thematic analysis. Thousand Oaks, CA: Sage Publications.

Herm, L.-V., Heinrich, K., Wanner, J. and Janiesch, C. (2023) 'Stop ordering machine learning algorithms by their explainability! A user-centered investigation of performance and explainability', International Journal of Information Management, 69, 102538.

Irani, Z., Abril, R.M., Weerakkody, V., Omar, A. and Sivarajah, U. (2023) 'The impact of legacy systems on digital transformation in European public administration: Lessons learned from a multi-case analysis', Government Information Quarterly, 40(1), 101784.

Khabouze, R. (2022) Modernization of Legacy Information Technology Systems. Doctoral dissertation. Walden University.

Klotz, S., Kopper, A., Westner, M. and Strahringer, S. (2019) 'Causing factors, outcomes, and governance of Shadow IT and business-managed IT: a systematic literature review', International Journal of Information Systems and Project Management, 7(1), Article 3.

Kopper, A., Fürstenau, D., Zimmermann, S., Klotz, S., Rentrop, C., Rothe, H., Strahringer, S. and Westner, W. (2018) 'Shadow IT and business-managed IT: A conceptual framework and empirical illustration', International Journal of IT Business Alignment and Governance, 9(2), pp. 53–71.

Kopper, A. and Westner, M. (2016) 'Towards a taxonomy for Shadow IT', in Proceedings of the 22nd Americas Conference on Information Systems (AMCIS).

Kvale, S. and Brinkmann, S. (2015) InterViews: Learning the Craft of Qualitative Research Interviewing. 3rd edn. Thousand Oaks, CA: Sage Publications.

Lakkaraju, S. (2025) 'Low-code/no-code integration platforms: Transforming digital innovation in banking', European Modern Studies Journal, 9(4), pp. 775–783.

Monaghan, B. and Bass, J. (2020) 'Redefining legacy: A technical debt perspective', pp. 1–16.

Nugraha, G., Munir and Dirgantari, P.D. (2025) 'Shadow IT transformation in the post-pandemic digital workplace: A systematic literature review', International Journal of Advanced Computer Science and Applications, 16(11), pp. 573–583.

Panko, R.R. (2006) 'Spreadsheets and Sarbanes-Oxley: Regulations, risks, and control frameworks', Communications of the Association for Information Systems, 17, pp. 647–676.

Raković, L., Sakal, M., Matković, P. and Marić, M. (2020) 'Shadow IT – A systematic literature review', Information Technology and Control, 49(1), pp. 144–160.

Shah, I.H. (2025) Robotic process automation in digital financial services: Operational efficiency, risk implications, and strategic integration. Working Paper. University of Lahore, Pakistan.

Silic, M. and Back, A. (2014) 'Shadow IT—A view from behind the curtain', Computers & Security, 45, pp. 274–283.

Spivey, T.D. and McIlveene, T.R. (2024) 'Navigating the shadows: A comprehensive framework for anticipating, identifying, and managing Shadow IT', ISACA Journal, 6, pp. 33–37.

Staron, M. (2025) 'Guidelines for conducting action research studies in software engineering', International Journal of Software Engineering and Knowledge Engineering, 19(1), pp. 1–19.

Yeo, K.S. and Megargel, A. (2024) 'Low/no-code and traditional code integration in digital banking', Journal of Digital Banking, 9(2), pp. 172–188.

Yin, R.K. (2009) Case study research: Design and methods. 4th edn. Thousand Oaks, CA: Sage Publications.

Zimmermann, S., Rentrop, C. and Felden, C. (2014) 'Managing shadow IT instances: A method to control autonomous IT solutions in business departments', in Proceedings of the Americas Conference on Information Systems.

Zimmermann, S., Rentrop, C. and Felden, C. (2017) 'A multiple case study on the nature and management of shadow information technology', Journal of Information Systems, 31(1), pp. 79–101.