RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

Modernizing legacy systems and IT governance in financial institutions: an analysis of Robotic Process Automation (RPA) and digital compliance.

Legacy systems modernization and its governance in financial institutions: an analysis on robotic process automation (RPA) and digital compliance

Vinicius Pereira Lensyk - Holds a degree in Management Processes from the International University Center (UNINTER). Specialist in Systems Analysis, IT Governance, and Business Process Modeling in Financial Environments.

Summary

The long-term viability of financial institutions in the digital economy intrinsically depends on their ability to overcome technological obsolescence without compromising data integrity and regulatory compliance. This scientific article proposes an exhaustive and multidisciplinary investigation into the challenges of modernizing legacy systems in banking environments, focusing on the application of *Robotic Process Automation* (RPA) and the structuring of IT governance frameworks. The methodology adopted is based on a narrative literature review, correlating Hammer's (1990) process reengineering postulates with the COBIT 2019 governance guidelines and the ISO 27000 family of information security standards. The study is structured around five high-density thematic axes, dissecting aspects ranging from the architecture of legacy systems and their operational risks, the strategic implementation of RPA for efficiency, digital *compliance* management and data protection, system integration via APIs and microservices, to strategic Business *-IT Alignment.* Theoretical results demonstrate that modernization is not merely a *software update,* but a restructuring of processes that, when well-managed, reduces operational costs (OPEX) and mitigates systemic risks. It is concluded that the business analyst acts as the architect of this transformation, ensuring that technological innovation is subordinated to the strategic and regulatory objectives of the institution.

Keywords: IT Governance. Legacy Systems. RPA. Digital Compliance. Management Processes.

Abstract

The longevity of financial institutions in the digital economy intrinsically depends on the ability to overcome technological obsolescence without compromising data integrity and regulatory compliance. This scientific article proposes an exhaustive and multidisciplinary investigation into the challenges of modernizing legacy systems in banking environments, focusing on the application of Robotic Process Automation (RPA) and the structuring of IT governance frameworks. The adopted methodology is based on a narrative literature review, correlating Hammer's process reengineering postulates (1990) with COBIT 2019 governance guidelines and the ISO 27000 family information security standards. The study is structured into five high-density thematic axes, dissecting everything from the architecture of legacy systems and their operational risks, the strategic implementation of RPA for efficiency, digital compliance management and data protection, system integration via APIs and microservices, to the Strategic Business-IT Alignment. The theoretical results demonstrate that modernization is not merely a software update, but a restructuring of processes that, when well-governed, reduces operational costs (OPEX) and mitigates systemic risks. It is concluded that the business analyst acts as the architect of this transformation, ensuring that technological innovation remains subordinate to the institution's strategic and regulatory objectives.

Keywords: IT Governance. Legacy Systems. RPA. Digital Compliance. Managerial Processes.

1. Introduction

The technological architecture that underpins the global financial system faces, in the 21st century, a structural paradox of critical and systemic proportions: the pressing, vital, and urgent need

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

Agile innovation to meet the volatile demands of a digitized consumer collides.
directly confronting the rigidity, hermetic complexity, and functional obsolescence of the systems.
Legacy *mainframes* still process the vast majority of global banking transactions.
In this scenario of profound dichotomy between the static architecture of legacy systems and fluid functionality
In the new context, Management Processes and Systems and Business Analysis emerge not as
Peripheral support functions, but as core and strategic disciplines for survival.
Institutional in a Darwinian market. The specialized academic literature, anchored in authors
Seminal works such as Laudon & Laudon (2014) and Weill & Ross (2004) strongly suggest that the
The simple overlay of modern digital interfaces onto archaic processing cores creates
an unsustainable technical debt, resulting in cybersecurity vulnerabilities.
Chronic operational inefficiency and inability to adapt to agile regulatory changes. Therefore, the investigation
rigorous scientific research on methodologies that allow for a safe, governed, auditable transition and
The efficient management of these complex environments becomes a topic of academic and pragmatic relevance.
urgent for software engineering and modern management of technological resources.

The central problem guiding this extensive, detailed, and profound theoretical analysis lies in
technical complexity of modernizing critical financial processing infrastructures without
interrupting business continuity *without* violating the strict, punitive, and
complex regulatory frameworks imposed by government entities, central banks, and standards
international financial *compliance .* The central hypothesis defended and dissected in this study is that
the strategic adoption of automation technologies, specifically *Robotic Process Automation.*
(RPA), combined with a robust, documented, and disciplined IT Governance framework (such as
COBIT (and the complementary frameworks ITIL and CMMI) offers the safest and most viable path.
for incremental and sustainable modernization. The structure of this article aims to dissect
meticulously examine the technical and managerial mechanisms by which business analysis identifies
Bottlenecks in repetitive manual processes are addressed by intelligent automation, ensuring integrity.
The mathematics of data in the migration from monolithic systems to distributed architectures. Throughout
In the following sections, it will be demonstrated with academic and methodological rigor how the application
Business Process Modeling (BPMN) concept technique, in-depth information security.
Microservices architecture allows financial institutions to transcend limitations.
Legacy physicals, transforming IT from a passive cost center into a driver of advantage.
Competitive, sustainable, auditable, and resilient.

2. Legacy systems architecture and operational risk management

The resilient and problematic persistence of legacy systems in the financial sector is not a
A historic accident, but the result of decades of massive investment in robust platforms, generally

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

based on languages like COBOL and other legacy technologies, which offer stability.
Transactional efficiency and unparalleled data consistency, however, at a cost to maintenance and integration.
and increasingly prohibitive and risky evolution. A deep, technical and structural analysis of this
The architecture reveals a gigantic monolith of data and business rules intertwined in a way that...
inextricable, where the modification of a simple routine for calculating compound interest or rates
Bank failures can trigger catastrophic cascading failures in critical accounting modules.
Federal regulatory reports and end-customer service interfaces. Operational risk.
An inherent and growing problem in these systems lies in the demographic scarcity of skilled labor for
maintaining them and the existence of a "black box" of business rules that are often not
documented in manuals, residing only in source code compiled decades ago and in memory.
tacit acceptance of employees nearing retirement. Process management, in this context, should begin-
if necessarily through archaeological work using software and reverse engineering, mapping the
Data flows and logical dependencies must be carefully considered before any migration or refactoring attempt.

The negative impact of these rigid systems on business agility is severe and measurable;
The *time-to-market* indicator for new financial products is drastically increased and negatively impacted.
due to the need for manual and exhaustive regression tests and the technical difficulty of exposing
legacy functionalities through modern RESTful or SOAP API interfaces. Furthermore, the
Information security in legacy systems is often based on perimeter paradigms.
obsolete, based on the flawed premise that the internal network is secure and reliable, a paradigm
which fails catastrophically against advanced persistent threats (APTs), ransomware
modern times and the imperative need for open data via *Open Banking.* Modernization,
Therefore, it is not just a matter of economic efficiency, but of urgent risk mitigation.
Cyber and operational issues that can lead to insolvency or regulatory intervention. The literature
Software engineering scholars, notably Pressman (2016), suggest that the encapsulation strategy,
where the legacy system is maintained as a stable *backend* while its functions are exposed via
Layers of abstraction are a valid intermediate step, but they don't solve the debt problem.
The underlying technique and horizontal scalability required for peak processing in the era
digital.

Governing these hybrid and complex environments (legacy + modern) requires control.
rigorous and disciplined approach to the application lifecycle management (ALM) and configuration management.
Flawless software to prevent version discrepancies and loss of integrity in environments.
production. The business and systems analyst must act as a bilingual translator across the limitations
Hostile *mainframe* techniques and the requirements for fluid user experience *(UX)* platforms.
Mobile and web digital technologies. The application of international risk management frameworks, such as ISO.
31000, allows for the mathematical quantification of the financial and reputational impact of failures in these areas.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

systems, justifying the massive capital investments to the boards of directors.
(CAPEX) required for its replacement or gradual upgrade. The strategy of
" *Strangler Pattern,* " conceptualized by Fowler (2004), where new functionalities
They are built exclusively on new modular platforms, whereas the old system is...
Gradually deactivated function by function, it presents itself as the safest methodology and
Recommended, but requiring rigorous project management discipline and a vision.
long-term architectural design that many organizations struggle to maintain.

Exhaustive and standardized process documentation (BPM) is the fundamental tool and non-negotiable to mitigate the risk of undocumented tacit knowledge residing in teams of Outdated IT. In many traditional financial institutions, vital business rules are "in the "Head" of former employees or "hardcoded" obscurely into the system, without documentation. Associated functional. The detailed survey and graphical modeling of these processes in notation. international standards (BPMN) allow the organization to regain intellectual control over its operations, identifying redundancies, performance bottlenecks, and optimization opportunities beforehand. automation or migration. Without this exhaustive and analytical mapping, the modernization attempt There is a very serious risk of simply "automating the chaos," perpetuating procedural inefficiencies in a more expensive and complex technological platform. Business analysis, therefore, precedes the Technology; it is the logical guarantee that the new systemic architecture will reflect real needs. and the institution's current situation, not just the limited capabilities of the acquired software tool.

Finally, operational risk management in legacy systems also involves planning. Strategic business continuity and disaster recovery (BCP/DR) in scenarios of Technological or physical catastrophe. Dependence on proprietary, obsolete, and unsupported hardware. The manufacturer creates a single point of failure that can paralyze operations . national banking systems and generate systemic chaos. The planned migration to cloud infrastructures. Public, private, or hybrid *cloud computing ,* although complex due to latency issues. Network and sovereignty of sensitive data, offering elastic resilience and geographic redundancy. impossible to replicate in traditional on-premises *data centers* at viable costs. The role of governance. The IT role is to orchestrate this delicate transition, ensuring that agreed service levels (SLAs) are met. maintained and that the ACID transactional integrity (Atomicity, Consistency, Isolation and Durability) — the most valuable asset of a bank — must be preserved intact at every stage of the process. technological modernization process.

3. Robotic process automation (RPA) as a driver of efficiency and auditing.

The disruptive technology of *Robotic Process Automation* (RPA) has emerged on the scene. global corporate solution as a high-impact, low-friction tactical solution to bridge the gap.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

operational gap between hermetic legacy systems and the need for agile digital processes and integrated, operating at the user interface layer to automate repetitive tasks, based based on logical rules and high transactional volume. Unlike traditional *backend integration,* which It requires the complex, time-consuming, and risky development of APIs and deep code changes. Using legacy sources, RPA simulates human action on the computer, interacting with multiple applications. heterogeneous (ERP, spreadsheets, websites, 3270 terminals, emulators) in a non-invasive and superficial. For financial institutions, this represents the revolutionary ability to automate Critical *back-office* processes — such as mass bank reconciliation, registration, and validation of Customer service, processing of payroll loans, and generation of complex regulatory reports. — with a speed, consistency, and precision unattainable by human labor, freeing up the valuable intellectual capital of employees for analysis, strategy and activities. relationship.

However, the strategic implementation of RPA requires a rigorous process analysis. Critical and corrective to avoid the dangerous automation of pre-existing inefficiencies. The principle The fundamental principle of "optimizing and standardizing before automating" is mandatory for the project's success. The business analyst must break down the target process into its elementary tasks, identifying the Binary logical decision rules and handling business exceptions before coding the robot. The literature specialized work by Willcocks and Lacity (2016), corroborated by studies on financial applications. (Moffitt et al., 2018) highlights that the sustainable success of RPA depends less on the technology than Automation itself, and more so corporate governance, regarding what is automated and how it is maintained. Poorly designed robots or those lacking error handling can replicate failures on an industrial scale. to fail silently in the face of minor changes to the graphical interfaces of legacy systems, creating a gigantic hidden operational liability. Therefore, the creation of a Center of Excellence (CoE) in RPA is vital for standardizing development and monitoring the execution of robots in real time. Real-world and manage the maintenance lifecycle of automation systems.

In addition to operational efficiency and cost reduction, RPA plays a crucial role and often underestimated in internal auditing and regulatory *compliance .* Every action taken by The digital robot is recorded in detailed, timestamped *logs ,* creating an immutable audit trail. granular and 100% traceable for auditing purposes. In sensitive and high-risk processes, such as verification of international sanctions lists (OFAC), and prevention of money laundering (AML). or the validation of documents for opening accounts *(KYC - Know Your Customer),* the accuracy The algorithmic and deterministic nature of the robot eliminates human error due to fatigue and the risk of internal fraud. Collusion. Automation mathematically guarantees that *compliance* policy is executed. strictly as designed and approved, without subjective deviations or operational omissions, providing robust legal security for the financial institution in the face of regulators.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

state-owned companies and independent external auditors.

The elastic scalability of the digital workforce provided by RPA allows that institutions deal with seasonal demand spikes or unforeseen market events without... The need for costly hiring and training of temporary workers. Software robots. They can work 24 hours a day, 7 days a week, 365 days a year, without breaks, vacations or pay. labor-related, drastically increasing processing capacity (throughput) and availability. of the organization. However, managing this hybrid digital workforce requires new IT and business skills. It is necessary to monitor the "health" and performance of the robots, manage the access credentials and secrets (password vault security) and orchestrate the work queue for ensure that the most critical and time-sensitive processes are prioritized for execution over Lower-value routines. Systems analysis must evolve to understand interdependencies. complex interactions between bots, data, and underlying systems, preventing software updates. Third-party companies break down automation systems in production.

The advanced integration of RPA with emerging cognitive technologies, such as Intelligent Optical Character Recognition (OCR), Natural Language Processing (NLP) and Artificial Intelligence (AI) expand the scope of automation to processes involving unstructured data and probabilistic decisions, such as reading and interpreting contracts. Legal documents, client emails, and document images. This evolution, called *Intelligent Automation* (AI), or Hyperautomation, allows the system to make decisions based on learning. supervised machine, forwarding only complex exceptions for human analysis or ambiguous. This symbiosis between machine and human maximizes operational efficiency and raises the level. Customer service level agreement (SLA), enabling faster, more accurate, and personalized responses. The role of A process manager's role is to strategically identify opportunities where this hybrid intelligence can be applied. It can generate greater added value and competitive advantage.

Finally, the financial analysis of the return on investment (ROI) in RPA projects should... Consider not only the reduction of *Full-Time Equivalent* (FTE) and payroll costs, but also also the mitigation of operational risks, the improvement of master data quality and speed. execution *(throughput).* Successful and well-governed automation projects often They pay for themselves in less than 12 months, but require ongoing investment in governance. Infrastructure and evolutionary maintenance. Technology is not "install and forget"; it's a capability. Organizational dynamics that must be managed as a long-term strategic asset. harmonious convergence between business process analysis, automation engineering and Corporate strategy is the critical factor that determines whether RPA will be a palliative tactical solution. short-term or a long-term structural strategic transformation for the financial institution.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

4. IT governance, data protection and digital compliance

Information Technology (IT) governance in modern financial institutions.
It transcends mere technical management of infrastructure and support to become a central pillar and
inseparable from corporate governance, essential to ensure that the substantial investments in
Technology generates tangible value, and the associated cyber and operational risks are...
mitigated to acceptable levels. The international COBIT 2019 framework establishes that governance
IT must strategically align with business objectives, ensuring the delivery of benefits.
Risk and resource optimization, and transparency for stakeholders. In an environment of
With accelerated digital transformation, where data is the most valuable and vulnerable asset, data governance
becomes critical and mandatory. Establishing clear institutional policies is imperative.
auditable aspects regarding the ownership, quality, accessibility, retention, and security of data to
throughout its entire life cycle, from capture at the source to legal archiving or disposal.
Safe and certified.

Strict compliance with data protection and privacy laws, such as the Law
The General Data Protection Law (LGPD) in Brazil and the GDPR in Europe impose technical requirements.
Strict legal and procedural rules apply to banks and fintechs. The concept of *Privacy by Design* requires that...
Privacy and security should be incorporated into the architecture of systems and processes from their inception.
initial conception, and not as a later addition or superficial layer. This implies that
Technical implementation of advanced data anonymization and pseudonymization mechanisms.
Granular role-based and needs-based access control (RBAC/ABAC) and robust encryption
of data at rest (databases, backups) and in transit (networks, APIs). The systems analyst
Businesses must have the expertise to translate these complex legal requirements into specifications.
Functional techniques and systemic business rules, ensuring that the software not only works,
but that it operates strictly within the limits of legality, respecting consent and the
rights of the data subject.

Digital compliance in financial institutions *also* involves mandatory adherence to
Specific and rigorous sectoral regulations, such as those of the Central Bank and the Council.
National Monetary Policy Committee on cybersecurity, service outsourcing, and cloud computing.
The institution must demonstrate proven capability for continuous threat monitoring.
Cybersecurity, proactive management of software and hardware vulnerabilities, and tested response plans.
to security incidents. The implementation of a Security Operations Center (SOC)
operating 24/7 and using SIEM *(Security Information and Event Management)* tools
Correlating events is mandatory for detecting and responding to attacks in real time before they occur.
to prevent data breaches. IT governance must ensure that these security controls are in place.
Do not stifle the agility and innovation of the business; seek a dynamic and intelligent balance.

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

between protection and usability, where security is seen as an enabler of digital business.
reliable and lasting.

Identity and Access Management (IAM) is a
A critical and fundamental component of security in modern distributed and legacy systems.
centralized. With the proliferation of digital channels, open APIs, and hybrid remote work, ensuring
It is unequivocally clear that "who's who" and "who can do what" is a technical and procedural challenge.
complex. Implementing adaptive multi-factor authentication (MFA) and automated management
of the identity lifecycle (employee admission, job promotion, and termination)
They must be rigorously audited to prevent orphan accounts and excessive privileges. Failures in this
These processes are the main gateway for internal fraud, data leaks, and attacks.
Social engineering. Governance should establish policies for periodic access reviews.
(recertification), guaranteeing the principle of least privilege , where each user or
The system only has access to what is strictly necessary for the performance of its function.

Independent and regular systems audits are the final line of defense that validates effectiveness.
and adherence to IT governance. Internal and external auditors thoroughly examine the
IT general controls (ITGC), physical and logical security, and application controls to ensure
the integrity, availability and confidentiality of financial statements and compliance
Regulatory. Automation of internal controls and automatic generation of audit evidence.
They significantly reduce the cost, time, and friction of these verification processes. The analyst
Business leaders should design systems and processes that are "audit *by design".*
with detailed logs, protected audit trails, and full traceability of financial transactions
and administrative. The transparency and *accountability* provided by good governance.
They increase the confidence of investors, regulators, and customers, reducing the cost of capital and risk.
reputational damage to the institution.

In conclusion, within this thematic area, it can be seen that IT governance and information security are not...
These are bureaucratic barriers to innovation, but they are also indispensable structural foundations. Without a
With a robust, mature, and integrated control structure, the speed of digital transformation can lead to...
A financial institution is at risk of irreversible operational, financial, or reputational collapse. Integration
cultural and procedural interaction between the areas of risk, *compliance,* information security, legal and
Systems development (DevSecOps), aligned with the principles of Kim et al. (2016), is
fundamental to creating an organizational culture of shared responsibility, where the
Security and compliance are an intrinsic responsibility of everyone, from the developer to...
junior code leaders up to the CEO level, ensuring institutional resilience in the face of threats.
of the 21st century.

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

5. Strategic alignment of business and IT and microservices architecture

Strategic Alignment between Business and Information Technology *(Strategic Business-IT Alignment* is considered the "Holy Grail" of modern corporate management, referring to the degree of harmony and integration in which the IT mission, objectives, and plans support, drive, and are supported by the mission, objectives, and strategic plans of the business. In financial institutions, where the product being sold is essentially digital (bits and bytes representing monetary value and (contractual), this alignment is not optional, but existential. The lack of synchronization between the areas This results in the phenomenon of "Shadow IT" (business areas contracting technological solutions without proper authorization). (official IT), massive waste of financial resources on projects that do not generate added value. and irretrievable loss of market opportunities due to technological lag *(Time-to-Market)* (high level). The role of the Senior Business Analyst and Process Manager is to act as the link to diplomatic and technical liaison , translating the abstract corporate strategy into a *roadmap.* concrete technological solutions, ensuring that IT is proactive and innovative in proposing solutions that... Enable new business models.

The transition from the monolithic, rigid, and coupled architecture of legacy systems to a Modern, flexible, and decoupled architecture based on microservices is the most significant technical manifestation. This strategic alignment is clearly aimed at achieving agility and scalability. Microservices They allow specific banking functionalities (e.g., balance inquiry, PIX transfer, calculation). Credit scoring, invoice issuance) should be developed, implemented, updated, and scaled. It operates independently, without affecting the rest of the ecosystem. This provides tactical flexibility. This is enormous for the business, allowing them to launch new *features* and fixes in days or weeks, instead of... typical mainframe cycles of months . The adoption of APIs *(Application Programming Interfaces)* Standardized and secure solutions facilitate seamless integration with external partners, startups, and fintech companies. enabling the *Banking as a Service* (BaaS) business model and active participation in The competitive ecosystem of *Open Finance.*

The management and orchestration of this distributed and granular architecture, however, introduces a significant operational and monitoring complexity that did not exist in the monolithic world. Container orchestration (e.g., Kubernetes), service mesh management , as discussed by Calcote and Butcher (2019), and distributed observability (logs, metrics and tracking) become essential technical skills for the infrastructure and operations team. Strategic alignment requires that the decision to break up a monolith into microservices be... based strictly on business domains (DDD - *Domain-Driven Design),* as proposed by Evans. (2003), and not just in technical preferences or technological fads. The analyst must map precisely define the bounded contexts *of* the business to ensure that the boundary The software services faithfully reflect the operational reality and ubiquitous language of

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

organization, avoiding excessive coupling that would negate the agility benefits of
modularization.

DevOps culture and the adoption of agile development methodologies (Scrum, Kanban,
SAFe refers to the organizational processes that operationalize this alignment in the day-to-day operations of...
Product teams. The collaborative and continuous approach between development teams.
(Development) and operations (Ops), combined with short delivery cycles (sprints) and continuous customer feedback.
Finally, it ensures that the software product evolves in close alignment with real and changing needs.
from the market. IT project portfolio management should prioritize value-based initiatives.
Measurable and auditable business *value,* using financial metrics as value.
Net Present Value (NPV), Return on Investment (ROI), and Cost *of Delay* for
deciding where to allocate capital. Alignment is not a static state to be achieved only once.
but a dynamic, iterative and continuous process of constant adjustment between technological capabilities.
available resources and the organization's business ambitions.

Open innovation and strategic collaboration with the external ecosystem.
Fintechs and startups are natural extensions of modern strategic alignment. Banks
Traditional companies, however large they may be, cannot innovate with excellence on all fronts.
independently and at the speed demanded by the market. The ability to integrate third-party solutions from
A fast, secure, and transparent approach becomes a crucial competitive advantage. Governance of
APIs and the management of technology partnerships are becoming indispensable new business skills.
The business analyst must carefully evaluate, through *Make or Buy studies,* when
"Building in-house" and when to "buy, rent, or integrate" off-the-shelf solutions, considering
Total cost of ownership (TCO), implementation time, strategic control, and differentiation.
competitive. This holistic view avoids the "not invented here" syndrome and accelerates transformation.
digital version of the institution.

Finally, strategic alignment requires transformational and visionary leadership that
Foster a digital culture throughout the organization, from interns to the board of directors.
Technology should be demystified and understood by everyone not as a magical black box, but
as a logical tool for business empowerment. Continuous and cross-functional capacity building of
business teams on fundamental technological concepts and IT teams on concepts
Banking and finance professionals create a common language and a shared understanding that reduce
Friction is reduced, communication barriers are eliminated, and synergistic collaboration is enhanced. The success of
Banking modernization does not reside solely in the quality of the written code, but in the ability of
An organization learns, adapts, and aligns its technological resources with its vision for the future.
a cohesive, disciplined, and strategic approach.

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

6. Conclusion

The extensive, meticulous, and dense analytical and investigative journey undertaken throughout the sections. This scientific article allows us to consolidate, in a well-founded manner, the thesis that the modernization of legacy systems and the implementation of robust IT governance in non-financial institutions These are merely technical projects for updating technological infrastructure or compliance. not bureaucratic, but rather strategic imperatives for survival, resilience, and competitiveness in a The digital and globalized economic scenario was demonstrated through a narrative literature review. and from the in-depth conceptual analysis of architectural paradigms, that the inertial maintenance of Obsolete monolithic architectures represent an unacceptable and growing systemic risk, both because from the perspective of operational inefficiency and unsustainable maintenance costs, as well as from the perspective critical of cybersecurity, data integrity, and regulatory compliance required by regulatory bodies. The management of managerial processes, when instrumentalized by the analysis of professional business and cutting-edge information technology provides the methodological framework. necessary to break down the complexity of old systems and rebuild them on new foundations. Modern, agile, scalable, and auditable.

The strategic implementation of *Robotic Process Automation* (RPA) has proven, throughout the Detailed analysis, as a tactical tool of extraordinary power for the digital transition. Smooth and efficient. By automating the "bonding layer" between disparate systems and eliminating manual labor. Unlike repetitive manual processes, RPA not only generates immediate cost efficiencies and frees up valuable capital. Humans are suited for high-level analytical activities, but they also act as a powerful *compliance* vector. and auditing, mathematically ensuring that business rules and institutional policies are executed with precision, consistency, and complete traceability. However, technology alone is insufficient and dangerous if not managed properly; its effectiveness and safety depend inextricably linked to strict governance that prevents the uncontrolled proliferation of non-robots Managed *(Shadow RPA)* and ensure strict alignment with the security architecture of information and business objectives.

IT governance and data protection emerged in this investigation as the cornerstones of trust and legitimacy upon which the modern digital financial system is based. In a A landscape of sophisticated, persistent, and global cyber threats, and privacy regulations. With increasingly strict and punitive data regulations (such as the LGPD), the institutional capacity to demonstrate Effective control, continuous monitoring, and rapid incident response are vital for reputation and... The bank's continuity regarding its own financial solvency and liquidity. The architecture of Microservices and integration via standardized APIs, discussed within the context of alignment. Strategically, they have proven to be the fundamental technical enablers that allow banks Traditional companies are competing in speed, flexibility, and innovation with digitally native fintechs.

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

enabling new collaborative and open business models such as *Open Finance* and *Banking as a Service.*

Furthermore, the research demonstrated, in a compelling and cross-sectional manner, that the human factor, the Organizational culture and leadership are absolute determinants of success or failure. Technological modernization. The role of the Senior Business Analyst and the Process Manager. It stood out as the unifying and translating element capable of connecting the technical dialects of Software engineering aligned with the business's commercial and regulatory needs, mediating conflicts. Prioritizing and aligning delivery expectations. The adoption of agile methodologies and culture. DevOps is not just about procedural changes in work, but about profound transformations of... *A mindset* that demands visionary leadership and a long-term strategic vision. Continuous training. For teams, talent retention and the management of tacit and explicit knowledge are essential for to prevent technological modernization from resulting only in a new generation of legacy systems. incomprehensible and ungovernable in the near future.

Analysis of the evolution of banking systems has shown that technology is not an end in itself. In itself, but a powerful means to achieve efficiency, safety, and customer satisfaction. A Modernization should be viewed as a continuous journey, not a static destination. Institutions that understand this dynamic invest not only in software and hardware, but in... Process intelligence, enterprise architecture, and data governance. The ability to orchestrate Complex ecosystems, integrating robust legacy systems with new digital technologies, defines The agility and resilience of the financial institution. The balance between disruptive innovation and... Operational stability is a constant challenge that demands mature governance and IT management. aligned with business objectives.

Another crucial point raised by the study is the interdependence between modernization. Technological and economic sustainability of financial institutions. Reducing the total cost of Total Cost of Ownership (TCO) of IT systems, achieved through the decommissioning of expensive mainframes, Automating manual processes and migrating to the cloud frees up financial resources for Investments in innovation and new products. Operational efficiency generated by technology. Modern technology allows banks to offer more competitive services, with lower fees and better... user experience, ensuring its relevance in an increasingly commoditized market and contested. Business analysis provides the metrics and feasibility studies needed to Prioritize these investments and demonstrate the return to shareholders.

Therefore, based on all that has been presented and argued, it can be concluded that the future of Financial institutions' ability to orchestrate a metamorphosis undoubtedly resides in their capacity to do so. continuous, governed, and intelligent, where technology is fluid, processes are optimized, and... Governance is omnipresent. The epistemological, technical, and practical convergence between the Science of

Year V, v.2 2025 | Submission: 09/22/2025 | Accepted: 09/24/2025 | Publication: 09/26/2025

Computer science, business administration, and process engineering form the framework.

The intellectual capacity needed to face the complex challenges of the 21st century. Organizations that

They succeed in integrating the robustness and reliability of legacy systems with the agility and innovation of modern systems.

digital, under the aegis of ethical, transparent and efficient governance, not only survive the

Despite market turbulence, they are leading the reshaping of the global financial system. Modernization is...

Ultimately, a continuous process of evolutionary adaptation, guided by analytical intelligence.

human and empowered by the brute force of digital automation.

References

CALCOTE, Lee; BUTCHER, Zack. **Istio: Up and Running.** Sevastopol: O'Reilly Media, 2019.

COBIT 2019. **COBIT 2019 Framework: Introduction and Methodology.** Schaumburg: ISACA, 2018.

EVANS, Eric. **Domain-Driven Design: Tackling Complexity in the Heart of Software.** Boston: Addison-Wesley, 2003.

FOWLER, Martin. **StranglerFigApplication.** MartinFowler.com, 2004.

HAMMER, Michael. **Reengineering Work: Don't Automate, Obliterate.** Harvard Business Review, vol. 68, no. 4, p. 104-112, 1990.

ISO/IEC 27001. **Information technology - Security techniques - Information security management systems - Requirements.** Geneva: International Organization for Standardization, 2013.

Kim, Gene; DEBOIS, Patrick; WILLIS, John; HUMBLE, Jez. **The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations.** Portland: IT Revolution Press, 2016.

LAUDON, Kenneth C.; LAUDON, Jane P. **Management Information Systems: Managing the Digital Firm.** 13. ed. Boston: Pearson, 2014.

MOFFITT, Kevin C.; ROZARIO, Andrea M.; VASARHELYI, Miklos A. **Robotic Process Automation for Financial and Accounting Applications.** Journal of Emerging Technologies in Accounting, v. 15, no. 1, p. 1-10, 2018.

PRESSMAN, Roger S. **Software Engineering: A Practitioner's Approach.** 8th ed. Porto Alegre: McGraw-Hill, 2016.

WEILL, Peter; ROSS, Jeanne W. **IT Governance: How Top Performers Manage IT Decision Rights for Superior Results.** Boston: Harvard Business School Press, 2004.

WILLCOCKS, Leslie; LACITY, Mary. **Service Automation: Robots and the Future of Work.** Warwickshire: Steve Brookes Publishing, 2016.