HSLU Lucerne University of Applied Sciences and Arts

# The Future of Technology in Finance

**Roadmap for IT Architectures and Infrastructures**

Institute of Financial Services Zug IFZ
www.hslu.ch/ifz

finnova.

FINSTAR

inventxLAB
INNOVATION BY DESIGN

Kanton Zug

SFTI

SIX

Zürcher Kantonalbank

FH Zentralschweiz

# Contents

# 1. Introduction

The financial industry is undergoing a profound technological transformation. Advances in digital infrastructures, artificial intelligence, cloud computing, and data analytics are reshaping how financial services are designed, delivered, and regulated (KPMG, 2025). At the same time, growing competitive pressure from FinTech and BigTech companies, heightened regulatory requirements, and shifting customer expectations are challenging the resilience of traditional banking models (KPMG, 2023; Hess, 2024). In this dynamic environment, future information technology (IT) architectures and infrastructures are no longer merely operational backbones but have become key strategic assets that will determine the adaptability, efficiency, and competitiveness of financial institutions in the coming decade.

This report investigates the future of IT architectures and infrastructures in the financial sector. The analysis is structured around three main perspectives. First, it provides an overview of current architectures and infrastructures, including their core components and governance structures (Chapter 2). Second, it identifies and discusses the key requirements likely to shape future system designs, such as functionality, economic efficiency, security, flexibility, and data-driven capabilities (Chapter 3). Third, it outlines possible future evolutionary developments across the architectural layers (Chapter 4). Three revolutionary scenarios are also presented and examined in terms of their feasibility (Chapter 5).

Building on this framework, the primary focus of the report is on the Swiss banking ecosystem, which combines longstanding institutional traditions with strong exposure to technological innovation. The report considers not only Swiss banks but also FinTech companies that act as essential suppliers and innovation partners (Ankenbrand, Bieri, & Gattlen, 2025). Although the main emphasis lies on the Swiss context, international influences and global market participants are also selectively taken into account. This applies in particular to core banking system providers, whose platforms and services remain relevant to the digital backbone of Swiss financial institutions. Swiss banks operate diverse business models shaped by both tradition and global financial dynamics. Private banking and wealth management are typically more global in orientation, whereas retail banking tends to have a more national focus. At the same time, investment services and FinTech-driven innovations are gaining importance (Swiss Financial Innovation Desk, 2025). Regulatory shifts, increasing challenges in IT security, and greater global transparency are reshaping strategic priorities across the sector. Consequently, the processes and requirements of individual banks and banking groups vary considerably depending on their business models, reinforcing the need for IT architectures and infrastructures that are adaptable, resilient, and future-proof.

The analysis adopts a long-term perspective, examining how IT architectures and infrastructures may evolve over the next five to ten years. Given the uncertainty associated with this horizon, the aim is not to deliver deterministic forecasts but to identify fundamental trends and formulate development propositions. Inevitably, this broad perspective comes at the expense of granularity, yet it enables a structured discussion of strategic directions.

The motivation for this report is grounded in pressing industry challenges. On the one hand, banks are increasingly seen as constrained by costly and inflexible IT infrastructures (Blattmann, Buschor, & Ettlin, 2024; Murphy, 2025). On the other hand, regulatory and technological requirements are intensifying, particularly in the areas of cyber security, resilience, and artificial intelligence (FINMA, 2024; Federal Reserve, 2025). Core banking systems remain the backbone of existing IT architectures, yet their replacement has often been likened to open-heart surgery, as they are costly, risky, and marked by uncertain benefits for institutions and clients (Fischer & Dibbern, 2024). Against this background, the report aims to formulate propositions on long-term requirements and explore potential solutions from an ecosystem perspective.

# 2. Current IT Architectures and Infrastructures in Finance

Understanding the current state of IT architectures and infrastructures in finance is a prerequisite for assessing potential future developments. This chapter provides an overview of the architectural layers and technological components that constitute the backbone of contemporary financial institutions. Section 2.1 introduces the general framework, outlining its conceptual foundations and overall design principles. The following sections then examine the individual components of the framework in greater detail.

## 2.1. Architecture and Infrastructure Framework

A structured understanding of financial IT landscapes requires a comprehensive framework that captures both technological and organisational dimensions. For this purpose, the analysis in this chapter is based on the InventxLab reference architecture developed by Inventx (Rhyner, 2023b). The framework provides a blueprint for categorising the core elements of banking IT, ranging from customer-facing layers (i.e., the digital experience platform) to the underlying infrastructure and governance mechanisms.

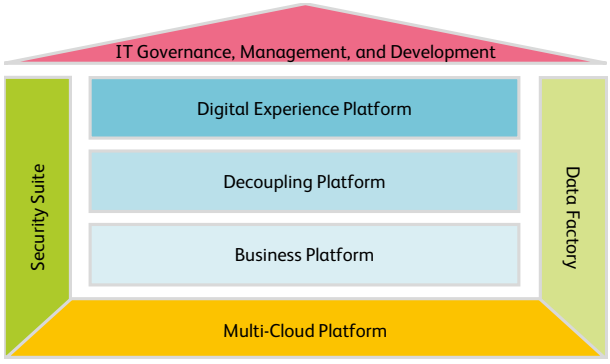


Figure 2.1: IT architecture blueprint. Source: Based on Rhyner (2023b)

Figure 2.1 illustrates this reference architecture. It depicts the principal layers and components that constitute modern financial IT systems, including the business platform, decoupling platform, digital experience platform, security suite, data factory, multi-cloud platform, and IT governance, management, and development. These elements interact to form an integrated architecture that supports both operational stability and innovation capacity.

The subsequent sections (Section 2.2 to Section 2.8) examine each of these components in greater detail, highlighting their current state, challenges, and implications for financial institutions.

## 2.2. Business Platform

The business platform encompasses the core functionalities required to realise a bank's business model. These include retail, commercial, and investment banking, as well as cross-cutting functions such as marketing and sales, risk and compliance, and business support. In most institutions, these functionalities are embedded in the core banking system, which serves as the central operational backbone. It processes banking transactions and updates accounts and financial records on a daily basis, and includes "deposit, loan, and credit processing capabilities, along with interfaces to general ledger systems and reporting tools" (Fischer & Dibbern, 2024).

Against this background, the Swiss core banking market is characterised by a limited number of established providers alongside emerging, cloud-native solutions from global software providers. The Swisscom Core Banking Radar highlights that established platforms such as Avaloq, Finnova, Finstar, Olympic, Temenos, and TCS BaNCS continue to dominate, while newer entrants like Thought Machine (Vault Core), Tuum, and Mambu are gaining attention due to their open design and modular, API-first architectures (Popp, 2023; Tunçer, Popp, Eckert, & Zerndt, 2025).[1]

Smaller retail banks in Switzerland predominantly rely on core banking solutions from Avaloq or Finnova (Popp,

[1] For an additional, though less current, overview of core banking systems, see the 2023 market overview by IT-Finanzmagazin, accessible here.

2023), which together account for the majority of this segment (Blattmann & Buschor, 2023). Some institutions also use Finstar or other niche providers (Blattmann & Buschor, 2023). Overall, these banks usually source their core application from a BPO provider that operates the system based on a shared platform and configuration. Consequently, they benefit from standardised systems that follow a "model bank" approach, ensuring that core functionality and security requirements are met at a reasonable cost. Mid-sized and larger retail banks also often rely on Avaloq's and Finnova's core banking solutions and use a higher level of individualisation. Depending on their specific requirements for functionality, flexibility, or security, however, other providers are also chosen. A few mid-sized retail banks operate with alternative or individually developed solutions. Large banks, such as UBS or Zürcher Kantonalbank, often rely more heavily on individual systems, adopt customised configurations of standardised platforms like Avaloq's implementation for Raiffeisen (Avaloq, 2019), or use entirely different solutions such as PostFinance with TCS BaNCS (Tata Consultancy Services, 2011).

Compared to more retail-oriented banks, smaller private banks use a variety of core banking solutions. These include Avaloq, Finnova, Finstar, and Tata Consultancy Services (TCS), which primarily cover basic functionality and security needs. Mid-sized and larger private banks, by contrast, face higher functional and security demands and therefore frequently rely on more advanced solutions, often from Avaloq, Finnova, Olympic, or Temenos.

Overall, the choice of core banking system largely reflects the size and strategic orientation of the institution. Large universal banks typically rely on highly customised platforms, whereas smaller institutions tend to adopt more standardised approaches. Beyond these structural differences, however, perceptions of core banking systems vary considerably between providers and banks. Providers generally assess the current state of core banking systems more positively than banks, which call for shorter innovation cycles, more flexible cost structures, and greater customer orientation. Although banks acknowledge the stability and functional breadth of existing platforms, they criticise their limited flexibility and long development times. The high effort and risk involved in switching systems creates strong dependency on providers, often described as a "lock-in effect". Such dependency can lead to strategic standstill, as all parties involved benefit from the status quo without real incentives for change. Neobanks, in particular, highlight the lack of digitalisation and advocate modular solutions, but face market-related hurdles and regulatory constraints (Blattmann, Buschor, & Ettlin, 2023).

These concerns are reinforced by the growing complexity within banks, particularly in large institutions, which is increasingly perceived as a burden and restricts their ability to expand service offerings. IT departments therefore advocate greater standardisation to better manage diverse requirements. The large number of peripheral systems, limited process harmonisation, and increasing licensing and maintenance fees imposed by global technology providers are major contributors to rising costs and obstacles to innovation. At the same time, core banking systems are often regarded as insufficiently open and modular, hampering flexible integration with other applications and limiting the agility of the business platform (Blattmann et al., 2023).

## 2.3. Decoupling Platform

The decoupling platform, also referred to as the integration layer, acts as a middleware connecting the core banking system (see Section 2.2) to other applications, services, and platforms. Its primary purpose is to enable secure data exchange, messaging, and process automation while ensuring that innovation and system changes can occur without directly affecting the underlying core system.

At the heart of this platform are application programming interfaces (APIs), which provide standardised, reusable, and secure interfaces between systems. By leveraging APIs, the decoupling platform unifies communication across different applications, such as between a customer relationship management (CRM) system or a data lakehouse and the core banking platform. This layer is particularly critical for front-end applications, which require frequent updates to meet evolving customer needs, whereas core banking systems typically evolve at slower speeds dictated by maintenance and release cycles. In addition, the decoupling platform functions as the technical handover point for Open Banking and Open Finance, where internal services are exposed externally in a controlled manner through standardised APIs. In this sense, it not only supports organisational decoupling but also acts as the gateway for banks to participate in broader ecosystems and to enable third-party innovations.

In addition to APIs, the decoupling platform integrates a range of supporting technologies. Job scheduling and management systems coordinate batch processes and background tasks, including account reconciliations, report generation, and large-scale data processing. Messaging and streaming technologies facilitate real-time data exchange between applications and services. Various tools support process orchestration, offering reusable workflows, microservices, and APIs that can be distributed through process marketplaces. Together, these components make the decoupling platform a critical enabler of flexibility, modularity, and innovation in modern banking IT architectures.

Beyond the intra-bank perspective, decoupling platforms increasingly play a role in inter-bank connectivity. Initiatives such as bLink illustrate how standardised API-based integration layers can facilitate secure and efficient communication between different financial institutions. By providing a shared decoupling and integration framework across banks, these platforms enable cross-institutional process automation, instant payments, and the creation of joint ecosystems (SIX, 2024). This development expands the scope of the decoupling concept: from supporting modularity and innovation within a single bank to fostering interoperability and collaborative service offerings across the entire financial industry.

## 2.4. Digital Experience Platform

The digital experience platform (DXP) represents the architectural layer closest to customers and many external partners. A DXP orchestrates multiple solutions and channels, aiming for a seamless digital customer journey (Shivakumar & Sethii, 2019; Gartner Peer Insights, 2025). Thus, all customer-centric technologies converge at this layer, including mobile and web applications, e-banking, content management systems, and social media integrations.

Mobile solutions such as smartphone apps are well established, provided by most banks, and have become the primary touchpoint for many institutions. By the end of 2022, approximately 62 percent of all banking logins in Switzerland were conducted via mobile devices, and in some institutions more than 80 percent of logins took place via smartphone (Dietrich & Amrein, 2024). Technically, these solutions are either individually developed or white-labelled from core banking providers or other third parties. Mobile banking solutions are mostly designed following a modular software architecture based on loose coupling and headless design[2], typically implemented via standardised APIs.

In 2023, web-based applications were still more widespread among banks than mobile banking solutions, with approximately 84 percent of the Swiss population using online banking (Eurostat (via Statista), 2024). Yet many banks still lag behind in adopting modern, responsive designs. Consequently, advanced developments such as the metaverse or mixed-reality environments are not currently considered strategic priorities. Among retail banks in Switzerland, only seven percent regard the metaverse as highly important, while 78 percent rate its importance as low or even non-existent (Blattmann, Fischer, & Ettlin, 2025).

Other relevant elements of the DXP include content management and social media tools, which are mainly used for marketing purposes but often remain only loosely integrated into core banking environments. Marketplace solutions are also gaining in importance as part of the ongoing evolution of Open Finance and Embedded Finance. However, these solutions are often designed outside of banks, for example, in the field of credit lending[3], yet they increasingly influence customer expectations regarding digital ecosystems.

Reflecting on the evolution of digital platforms, most banks have moved beyond the early evolution phase of merely providing websites as basic digital touchpoints (Shivakumar & Sethii, 2019). Instead, technology platforms with domain-specific features have been developed and deployed. However, the final stage, including a comprehensive personalised and user-centric customer experience based on an integrated, omnichannel platform, has not yet been reached by the majority of financial institutions in Switzerland.

---

[2] Loose coupling is an architectural principle stating that "components and services should have minimal dependencies on each other. Standardised, business-oriented APIs make sure consumers are not impacted by changes to services. This allows service owners to change implementation, switch out components, or modify data records behind the APIs without downstream impact to end users" (European Commission, 2025). Headless design extends this principle by separating front-end presentation from back-end logic, allowing banks to develop and adapt user interfaces independently of the underlying core systems.

[3] For more information on marketplace lending in Switzerland, see Berchtold, Amrein, and Dietrich (2025).

## 2.5. Security Suite

Building on these customer-facing and integration layers, the security suite constitutes a critical layer of the banking IT architecture, designed to safeguard sensitive financial data, preserve system integrity, and ensure resilience against internal and external threats.

The security suite also integrates advanced detection and prevention technologies. Extended detection and response (XDR) solutions monitor activities across systems to identify and respond to anomalies, while preventive measures such as data encryption and network micro-segmentation reduce the attack surface. In particular, micro-segmentation divides networks into isolated segments, limiting the ability of attackers to move laterally within banking systems.

These detection signals and preventive controls are centrally monitored and assessed in the security operations centre (SOC). SOC teams rely on security information and event management (SIEM) systems to collect and correlate events across diverse sources, enabling them to distinguish routine anomalies from actual security incidents and respond accordingly.

## 2.6. Data Factory

The data factory serves as the central platform for orchestrating the collection, integration, processing, and transformation of vast amounts of unstructured and structured data from diverse sources. Its purpose is to provide a reliable foundation for analytics, artificial intelligence (AI), machine learning, and business processes, forming the basis for data-driven operations.[4]

Clean and integrated data produced within the data factory enables the automation of routine processes through bots and other digital tools. These solutions rely on high-quality data inputs to operate efficiently and consistently. In addition, the platform aggregates and prepares data for use in business intelligence (BI) applications, which in turn generate dashboards and reports to support management decisions. Metadata management plays a crucial role in this context, as metadata documents data origin, quality, and lineage. This ensures transparency and accountability, both of which are essential for sound governance and regulatory compliance.

At the core of the data factory are the data warehouse (DWH) and data lake. The DWH stores structured, historical data optimised for query performance and BI reporting, while the data lake retains raw and semi-structured data at scale to support flexible analysis and innovation. The interplay of these components creates an environment where data science teams can access clean, comprehensive datasets for developing predictive models, as well as other advanced analytics, enabling personalised customer experiences and enhanced risk management strategies, for example.

## 2.7. Multi-Cloud Platform

A multi-cloud platform enables financial institutions to combine and manage IT infrastructure services from different cloud providers and deployment models, including private, community, and public clouds.[5] Its central function is to orchestrate and govern applications, data, and services across heterogeneous and distributed cloud environments. Effective platform management ensures regulatory compliance, monitors system performance, and optimises workload distribution across platforms. For secure, resilient, and highly available connectivity, software-defined (SD) networking and secure inter-domain routing with SCION[6] are common technologies.

The strategic relevance of multi-cloud management is steadily increasing as financial institutions push ahead with the adoption of emerging technologies. At the same time, regulatory requirements and third-party risk management (TPRM) considerations add further weight to

[4] See, for example, UBS Key4 Insights, which reports that after two years of operating its data-driven platform, UBS has generated millions of personalised "insights" (e.g., budget hints, spending alerts) through its analytics engine, positioning data as a core pillar of customer engagement (Dietrich, 2025).

[5] Private clouds are dedicated infrastructures for a single bank, often via providers like Swisscom or Inventx in Switzerland. Community clouds are shared by several banks to meet sector needs. Public clouds (e.g., Azure, AWS, or Google Cloud) offer scalability and efficiency but are adopted more cautiously in Switzerland (Blattmann et al., 2025).

[6] SCION (Scalability, Control, and Isolation On Next-Generation Networks) is a secure inter-domain Internet architecture developed in Switzerland. Unlike the current Internet's Border Gateway Protocol (BGP) routing, which connects autonomous systems but lacks strong security and path control, SCION offers cryptographic path validation, multi-path routing, rapid failover, and enhanced availability, reliability, and digital sovereignty (National Cyber Security Centre Switzerland, 2025).

the topic. Banks seek to avoid overreliance on individual cloud providers or hyperscalers and must demonstrate compliance with supervisory expectations regarding data portability, resilience, and credible exit strategies. Managing provider risks has therefore become a key element of sourcing strategies, with regulators and auditors demanding that institutions actively address concentration risks and ensure operational continuity across diverse cloud partners (Blattmann et al., 2025). Against this backdrop, the adoption of emerging technologies further reinforces the importance of multi-cloud infrastructures. Distributed ledger technologies (DLT) and blockchain solutions, for instance, often require interoperable environments across institutions, while the anticipated rise of quantum computing services is expected to further reinforce the need for flexible and secure multi-cloud platforms.

## 2.8. IT Governance, Management, and Development

IT governance, management, and development in banking have transformed in recent years from strong hierarchical structures to cross-functional or agile settings, reflecting the growing need for flexibility and responsiveness. Nonetheless, regulatory requirements continue to exert a significant influence. Governance processes, management decisions, and development activities are often subject to documentation and formalised oversight, ensuring compliance but also adding complexity to organisational structures.

Even before the rise of AI, banks had begun to transform their IT infrastructure from cost centres to strategic value-creating units. This shift has affected both organisational models and software development practices. A gradual technological transformation has started, moving from monolithic systems towards service-oriented architectures (SOA) built on microservices. At the same time, agile development methods and DevOps practices have reduced dependency on rigid release cycles, traditionally limited to two per year, by enabling more frequent and iterative software updates.

Consequently, IT and business functions are becoming increasingly interdependent. Shared value streams and agile teams require both domains to “speak the same language”, ensuring that technological development is directly aligned with strategic and operational priorities. In this way, IT governance, management, and development form a critical layer of the banking architecture, shaping how effectively institutions can adapt to regulatory, technological, and market-driven change.

# 3. Requirements for Future IT Architectures and Infrastructures in Finance

The design of future IT architectures and infrastructures in finance is driven by a set of interrelated requirements that extend beyond purely technical considerations. They reflect economic pressures, regulatory obligations, technological advances, and strategic priorities within the financial ecosystem. This chapter delineates five central requirements that are expected to shape the evolution of financial IT systems in the coming decade. These include:

- **Functionality**
- **Economic efficiency**
- **Security, compliance, and resilience**
- **Modularity and flexibility**
- **Data orientation and sovereignty**

Each requirement represents a distinct dimension of system design, yet their interdependencies highlight the complexity of modern financial IT. For example, achieving modularity may enhance flexibility but also raises challenges for security and resilience. Likewise, data-driven architectures offer opportunities for personalisation and automation while simultaneously intensifying demands for compliance and ethical use of information.

By systematically discussing these requirements, this chapter provides a framework for analysing both the shortcomings of current architectures and the guiding principles for future developments. This analysis serves as a conceptual bridge toward Chapter 4, where potential architectural solutions are outlined. The following sections (Section 3.1 to Section 3.5) examine each requirement in more detail.

## 3.1. Functionality

Functionality constitutes a fundamental requirement for banking solutions, as it defines the extent to which IT systems can support business models and enable innovation in processes, services, and products. From a customer or user perspective, it is of secondary importance whether functionality is delivered by a single system or through seamless integration and orchestration of loosely coupled software components. What matters is the availability, reliability, and orchestration of functions within the overall system landscape.

At its foundation, any financial IT architecture must provide essential capabilities to ensure stable and compliant operations, such as transactional processing, data management, and reconciliation (Fischer & Dibbern, 2024). Beyond these baseline functions, the ability to integrate and extend functionalities dynamically has become a key differentiator. For instance, advanced analytics, BI tools, and CRM systems enable institutions to generate insights, manage client relationships, and support data-driven decision-making. These may be embedded within the existing infrastructure or accessed through interoperable third-party solutions connected via APIs or decoupling platforms.

Equally important is functional accessibility and usability. Employees across business units, from relationship managers to compliance officers, rely on IT systems that present relevant functions and data in an intuitive and task-oriented manner. Modern architectures must therefore combine functional depth with simplicity of interaction, allowing users to operate efficiently and focus on value-creating activities rather than technical complexity. Functionality in this sense becomes a driver of both operational efficiency and strategic differentiation within the financial industry.

## 3.2. Economic Efficiency

Studies consistently confirm that economic efficiency remains an important topic for Swiss banks (Blattmann et al., 2025; Ernst & Young, 2025). It represents an essential requirement in any transformation project.

Two major cost dimensions are particularly relevant. The first concerns the initial investment and the associated transformation project. Depending on factors like the size of the bank and its maturity level regarding processes and data, the vendor's experience, or the core banking solution, the investment varies in magnitude. As an example,

Apobank in Germany spent about EUR 800 million for migrating to Avaloq's core banking solution (Gamma, 2021). Costs rise significantly when related tasks, such as process standardisation or data preparation, are incorporated into the project scope. In addition, the initial investment typically also covers expenses for the implementation of the new system and the training of employees, which are particularly essential to ensure successful adoption in daily operations.

The second cost dimension relates to necessary ongoing expenditures for maintenance, SaaS, licensing, and system support. These recurrent expenses must be weighed against the expected efficiency gains from modernising the IT infrastructure. As such, economic efficiency is not only a matter of upfront investment but also of ensuring long-term cost-effectiveness and scalability.

## 3.3. Security, Compliance, and Resilience

Security remains a top priority for Swiss banks and regulatory authorities, according to various studies (Blattmann et al., 2025; Ernst & Young, 2025). The frequency and sophistication of cyberattacks continue to increase, a trend amplified by technological advances, including the malicious use of AI. As a countermeasure, financial institutions require IT solutions that are not only secure but also resilient and stable, ensuring continuity of critical services under adverse conditions. Financial IT architectures must therefore integrate robust security measures such as encryption, granular access controls, and systematic security audits (Patel, 2024).

Security is not an isolated requirement but closely intertwined with other architectural dimensions. For instance, data management and system design are strongly affected by security considerations. Resilient architectures increasingly rely on concepts such as zero-downtime, self-healing infrastructures, and zero-trust principles to reduce vulnerabilities and ensure operational continuity.

Beyond technical safeguards, compliance remains a critical aspect. Financial IT architectures must support institutions in adhering to stringent regulatory standards, given that "security and compliance are non-negotiable in banking" (Day, 2024). This includes embedded processes, monitoring and logging functions, as well as adaptable workflows that facilitate regulatory reporting and adjustment to the new requirements. The provider's expertise in the relevant regulatory environment is therefore a significant factor in evaluating the security and compliance capabilities of a core banking solution.

In practice, compliance spans anti-money laundering (AML) and counter-terrorist financing (CTF), know-your-customer (KYC), data protection (e.g., GDPR, Swiss Data Protection Act), and prudential standards such as Basel III/IV. A modern IT solution must not only provide the technical infrastructure for these functions but also ensure traceability, auditability, and real-time monitoring to withstand regulatory scrutiny (Basel Committee on Banking Supervision, 2021). Increasingly, regulators demand integrated risk management frameworks, automated reporting, and capabilities to adapt swiftly to new supervisory requirements. Consequently, compliance is not merely an operational necessity but also a competitive differentiator in the evaluation and selection of an IT architecture and infrastructure.

## 3.4. Modularity and Flexibility

In an increasingly volatile and complex environment, financial institutions require IT systems that offer a high degree of adaptability. Flexibility in this context is closely linked to software architecture concepts such as modularity, configurability, and scalability. Together, these principles ensure that banks can tailor their core solutions to specific business models and adjust them as requirements evolve over time. As highlighted in the literature, this includes "the ability to support new products, services, and channels as the bank evolves" (Day, 2024). A key objective is to make software adaptations manageable and cost-effective, thereby avoiding "time-consuming, expensive, difficult-to-manage customisations" (Young, 2024). Providers must therefore design solutions that combine a robust functional foundation with broad configurability and seamless integration capabilities. Open APIs play a central role in this regard, enabling interoperability with third-party systems and preparing banks for Open Finance ecosystems.

Consequently, the IT architecture needs to be sufficiently agile to allow for scalability and open to new technologies, such as cloud-enabled solutions. In other words, "modern

approaches such as API-first strategies, agile work methods, DevSecOps[1] as well as microservices and application-containers improve the scalability and flexibility of systems, helping banks to adapt more quickly to changing market conditions" (Tunçer et al., 2025).

## 3.5. Data Orientation and Sovereignty

IT solutions fundamentally rely on the storage, processing, and exchange of data. As such, the thoughtful collection and management of data are critical requirements. Data integrity, defined as the consistency, accuracy, and reliability of data across all systems, is of particular importance in this respect. Without reliable data, neither regulatory compliance nor efficient business operations can be ensured.

Data constitutes a central asset for all banking activities, encompassing customer, financial, employee, process, and product information. Such data also serve as the basis for all regulatory reporting, thereby underpinning the importance of data consistency and the establishment of a "single source of truth". Institutions must ensure not only data completeness and consistency but also that critical data are managed with regard to confidentiality, integrity, and availability, as required in FINMA Circular 2023/1 (Operational risks and resilience – banks) (FINMA, 2022). The value of customer data in particular has grown substantially, as clients increasingly expect personalised services and tailored products. In parallel, advances in AI and related technologies have expanded the possibilities for data-driven personalisation, predictive analytics, and automation. Consequently, the "role of data in service design is becoming increasingly important" (Tunçer et al., 2025).

Beyond data integrity and orientation, data sovereignty has emerged as a key concern for financial institutions. Data sovereignty refers to the principle that digital information is subject to the laws and governance structures of the country in which it is collected, stored, and processed (Scherenberg, Hellmeier, & Otto, 2024). For banks, this implies that the location of data centres, the involvement of third-party providers, and cross-border data flows must be carefully managed to ensure compliance with national regulations such as the Swiss Data Protection Act, the EU General Data Protection Regulation (GDPR), or sector-specific supervisory requirements. In Switzerland, FINMA Circular 2018/3 on outsourcing stipulates specific conditions for outsourcing abroad, including contractual safeguards, monitoring obligations, and audit rights (FINMA, 2018).

Accordingly, sovereignty considerations extend beyond compliance to strategic questions of resilience, business continuity, and trust in the financial ecosystem. By enforcing oversight and monitoring requirements, regulators aim to ensure that institutions maintain effective control over critical data even when engaging external service providers (FINMA, 2018; European Central Bank, 2024).

[1] DevSecOps (development, security, and operations) integrates security into all phases of the software development lifecycle, from design to deployment, as a shared responsibility (Red Hat, 2023).

# 4. Baseline Scenario and Roadmap

The evolution of IT architectures and infrastructures in finance cannot be separated from the underlying technological forces that shape the industry. Several studies highlight that AI, DLT, cloud computing, and quantum computing represent powerful drivers of change in the coming decade (Basel Committee on Banking Supervision, 2024; World Economic Forum, 2018, 2025a, 2025b).

The baseline scenario of future financial IT architectures and infrastructures, described in this chapter, assumes an evolutionary development of existing IT landscapes, in which architectures, infrastructures, and operating models are gradually modernised and expanded rather than fundamentally replaced. In contrast, the alternative scenarios in Chapter 5 explore more disruptive trajectories. The following sections describe the evolutionary scenario based on the framework in Chapter 2, and examine its implications for the requirements defined in Chapter 3. While the sections on the business platform (Section 4.1) and the decoupling platform (Section 4.2) address all identified requirements in detail, the subsequent sections (Section 4.3 to Section 4.7) focus on the most critical aspects to avoid redundancy and highlight the key differentiating factors. The chapter concludes with a roadmap (Section 4.8) outlining the transition from current IT infrastructures and architectures toward future solutions.

## 4.1. Business Platform

Within the baseline scenario, today's core systems are expected to evolve into more dynamic and modular business platforms that actively enable innovation, accelerated by drivers such as AI and DLT. While core functionalities such as payments, lending, deposits, investments, and general ledger operations will remain indispensable, their role is shifting from monolithic structures towards orchestrated, API-first modules that can flexibly integrate emerging technologies and ecosystem services (e.g., Open Finance). For many institutions, it is becoming increasingly evident that traditional core banking solutions need to transform to master strategic challenges of the future (Blattmann et al., 2023). Banks face mounting pressure at the customer interface, seek to participate in ecosystems, and aim to deliver embedded banking solutions for non-financial partners. Older IT landscapes can act as a constraint, hindering agile development and the integration of new solutions. Against this backdrop, the business platform of the future must function less as a static backbone and more as a continuously adaptable foundation that restores the strategic "fit" between banking IT and evolving market demands, thereby ensuring that regulatory requirements, new products, and customer-driven innovations can be fully supported (Blattmann et al., 2023).

As highlighted by the Swisscom Core Banking Radar, most Swiss banks follow an evolutionary path of modernisation, gradually enhancing existing systems with modular components and open interfaces rather than replacing them entirely (Tunçer et al., 2025). Building on this observation, the current landscape can be broadly divided into two categories, i.e., established and neo core banking platforms, each reflecting a distinct level of technological maturity and strategic positioning.

**Established core banking platforms**, including Avaloq, Finnova, Temenos, Olympic, Finstar, TCS BaNCS, IBIS4D, and Sopra Banking Software, are long-standing systems with comprehensive functionality and proven compliance and stability. They form the operational backbone for most Swiss banks and include both major providers and smaller players with comparatively limited market shares. These platforms are deeply embedded in the country's financial infrastructure and continue to evolve through gradual modernisation efforts. By contrast, **neo core banking platforms** like Thought Machine, Mambu, Tuum, 10x Banking, and SaaScada represent a newer generation of systems. Built from the ground up with an API-first architecture, they prioritise modularity and scalability. However, they still lack adoption in the Swiss market.

Distinct patterns emerge when comparing these platform groups against the central requirements for future IT architectures as summarised in Table 4.1. In terms of **functionality**, established core banking platforms provide a comprehensive coverage across all banking processes and are considered mature, though the breadth of functionality may vary among providers. By contrast, neo core banking platforms focus on modular innovation and scalability, enabling the rapid addition of new features. However, certain areas, such as mortgage and investment services, are not yet fully tailored to the Swiss market.

Table 4.1: General comparison of core banking system types (the comparison may vary depending on the individual provider)

| Criteria | Established Core Banking Platforms | Neo Core Banking Platforms |
|---|---|---|
| **Description** | Established systems offering broad functionality, encompassing both major providers and smaller players with a comparatively limited market share in Switzerland. | Cloud-native platforms with an API-first architecture and a limited customer base in Switzerland. |
| **Functionality** | Covering all standard core banking processes, though functionality breadth may vary among providers. | Modular architecture allows the addition of new features, though some functional depth is still limited and not yet fully tailored to the Swiss market. |
| **Economic Efficiency** | High costs for maintenance and transformation (unless using standard versions), though efficiency gains arise through scale effects on the provider side and cost-sharing among banks. Cost levels vary across providers and banks. | Standardised SaaS/cloud models, lower fixed costs, and pay-as-you-grow scalability. |
| **Security, Compliance & Resilience** | Strong and regulatorily proven, but sometimes complex to adapt when addressing new requirements. | Cloud-native security, though regulatory frameworks are still evolving. A lack of Swiss-specific adaptations (“Swiss finish”) requires additional local adjustments. |
| **Modularity & Flexibility** | Monolithic structures, standardisation, and broad customer bases limit flexibility. Smaller client bases allow greater agility. | Standard API-first and microservice-based architecture offering adaptability to new technologies and market trends. |
| **Data Orientation & Sovereignty** | Legacy data models and historically grown data structures make integration complex. | Data-centric architectures with native cloud analytics and data lakes, though data sovereignty challenges remain. |

Regarding **economic efficiency**, established core banking platforms remain costly to maintain and transform, especially when customised beyond standard versions (Blattmann et al., 2023), yet they benefit from economies of scale on the provider side and cost-sharing among participating institutions. Cost levels may vary across providers, with smaller players typically benefiting less from such scale effects. Compared to established systems, neo core banking platforms aim to achieve greater economic efficiency and lower total cost of ownership (TCO) (Swisscom, 2023). They rely on standardised SaaS and cloud models, characterised by lower fixed costs, usage-based pricing, and flexible scalability.

For **security, compliance, and resilience**, established providers are regulatorily proven and robust, whereas neo core banking platforms integrate advanced, cloud-based security but still face challenges in implementing country-specific regulatory and compliance standards.

When considering **modularity and flexibility**, the differences between platform types are pronounced. Most established providers are constrained by monolithic architectures and large customer bases that make change processes slow and complex. However, smaller providers within this group, while partly monolithic, benefit from narrower client bases that allow greater agility and faster adaptation. At the same time, established vendors are increasingly introducing microservice principles and modular extensions to decouple legacy components and enable gradual modernisation (Tunçer et al., 2025). Neo core banking platforms, in turn, are designed with inherent flexibility, featuring API-first and microservice-based architectures that enable continuous integration of new technologies and services (ti&m, 2023).

Finally, with respect to **data orientation and sovereignty**, established systems continue to rely on legacy data models and historically grown data structures that make seamless integration difficult (Merlini et al., 2023). In contrast, neo core banking platforms are built around modern, data-centric architectures with native analytics and data lake capabilities. Nevertheless, questions of data

sovereignty remain particularly relevant for these systems, given their reliance on international cloud environments (Swiss Bankers Association , 2025).

In the baseline scenario, Swiss banks can therefore pursue different paths at different speeds, but all will need to ensure that their business platforms evolve into adaptable, interoperable, and future-proof foundations for innovation. Rather than large-scale migration waves, the transformation is expected to take place through gradual, evolutionary development. Established institutions will modernise progressively across individual architectural layers, for example, expanding their decoupling platforms toward inter-institutional integration and Open Finance connectivity. Emerging players, new market entrants, or specific use cases may also utilise neo core banking platforms.

For banks and core banking providers, this means they must continuously implement innovations and modern architectures to minimise the risk of customer attrition and, by extension, the potential for disruption. In the Swiss banking market, however, the disruptive potential has remained relatively limited due to two key factors: first, core banking transformations have historically proven to be highly complex and costly; second, for neo core banking platforms, it is often not economically viable to replicate the full scope of banking functionality for the comparatively small Swiss market, even if they possess cutting-edge, radically innovative systems. Consequently, as long as traditional banks and core banking software vendors continue to evolve and modernise their platforms, the risk of disruption is expected to remain contained.

## 4.2. Decoupling Platform

In the baseline scenario, the decoupling platform serves as the strategic integration layer connecting core systems, internal applications, and external ecosystems. Rather than triggering large-scale migration movements, its evolution follows an incremental and evolutionary path. Step by step, banks extend and modularise their existing architectures, first by decoupling internal domains, then by opening controlled interfaces toward partners, and ultimately by enabling cross-institutional integration. In this sense, the decoupling platform forms the architectural backbone of modularity, interoperability, and secure openness, allowing institutions to innovate and collaborate without compromising the stability of their operational core (Deb, 2023; Shumsky, 2023).

Internally, the platform encapsulates legacy systems behind stable, domain-specific interfaces and exposes core functions such as payments, lending, or investments through APIs and event streams. This enables front-end and analytics systems to evolve independently, establishing a modular IT landscape. As architectures mature, microservices and service meshes enhance observability, policy enforcement, and zero-trust communication, while governance mechanisms for APIs, contracts, and metadata ensure consistency and compliance. Many institutions pursue this transition gradually by segmenting their cores into modular “mini-cores” as illustrated by JPMorgan Chase’s Scalable Functional Aligned Services (SFAS) approach (Lodha, 2025).

Once internal modularisation is achieved, the decoupling platform becomes the gateway to Open Finance. Controlled APIs enable secure, consent-based data exchange with FinTech companies, insurers, and other partners. In Switzerland, initiatives such as SIX bLink exemplify this trend, demonstrating how middleware principles are being extended to inter-institutional interoperability.

In essence, the decoupling platform reflects the industry’s shift toward composable architectures, enabling back-end and front-end systems to evolve independently (Shumsky, 2023; Sivaganeshan, 2025). Building on this role, it is evaluated in the baseline scenario against the five key requirements for future financial IT architectures and infrastructures:

- **Functionality:** The decoupling platform provides the integration and orchestration capabilities that connect internal domains and external partners. Core functions include API gateway management, service mesh coordination, message transformation, event streaming, and interface monitoring. Consent, entitlement, and identity services ensure secure, policy-based data exchange and partner integration.

- **Economic efficiency:** By avoiding bespoke point-to-point connections and enabling incremental system upgrades, the decoupling platform reduces long-term IT complexity and integration costs. Shared components, such as gateways, logging,

and monitoring, create economies of scale across business units. While the initial setup and governance investment are substantial, the model supports sustainable cost efficiency and faster time-to-market for new services. However, growing architectural fragmentation can also increase coordination costs, as multiple specialised solutions require additional integration, data mapping, and orchestration efforts. Moreover, managing security, compliance, and vendor governance across a diverse provider landscape may offset some of the anticipated efficiency gains.

- **Security, compliance & resilience:** The platform enforces authentication and authorisation standards, encryption, and zero-trust networking. It provides audit trails, rate limiting, circuit breakers, and fallback mechanisms to ensure resilience. As the number of integrated components and interfaces increases, so do the security and compliance requirements. Ensuring consistent protection, monitoring, and incident response across a distributed architecture therefore becomes a critical success factor for the platform's stability and trustworthiness.

- **Modularity & flexibility:** The decoupling platform embodies modularity by design. It enables the independent evolution of front-end, middle-tier, and core systems, supporting parallel development and rapid integration of emerging technologies. Furthermore, it allows inter-institutional connectivity, forming the technical foundation for Open Finance ecosystems and new forms of collaboration across the industry.

- **Data orientation & sovereignty:** The decoupling platform's role in data management focuses on governance rather than analytics. It handles metadata management, interface-level logging, and cross-system auditability, ensuring traceable and compliant data flows. Data sovereignty remains anchored with each institution, as the platform mediates access through consent and purpose limitation rather than central data storage. In the context of Open Finance, data are becoming an increasingly valuable strategic asset, which further elevates the importance of robust governance, interoperability, and sovereignty frameworks at the platform level.

Overall, the decoupling platform emerges as the connective layer that bridges stability and innovation within banking IT. In the baseline scenario, its role evolves from a technical middleware to a strategic enabler of ecosystem participation. It ensures that legacy systems remain operable while new, data-driven, and modular services can be introduced in compliance with regulatory standards. This transformation is reinforced by FinTech and BigTech companies, which are increasingly entering the financial services market with payment, credit, and other embedded financial services. Over time, decoupling platforms will thus define how Swiss banks balance control and openness, offering the flexibility to innovate without compromising resilience or sovereignty.

## 4.3. Digital Experience Platform

Within the baseline scenario, the DXP functions as the core orchestration layer that enables seamless digital customer interactions. It links mobile, web, and social channels with core systems and ecosystem partners, enabling consistent and personalised experiences across touchpoints.

As institutions modernise, isolated digital channels are replaced by unified front ends built on shared design systems and data models. The DXP thus evolves into the bank's "front-end brain", coordinating content, transactions, and analytics in real time and integrating third-party offerings to deliver seamless, cross-sector experiences. Consequently, financial institutions are increasingly investing in integrated platforms that enable consistent, data-driven, and customer-centric digital experiences across their ecosystems (Swiss Fintech Innovations, 2018; DECTA, 2025; L'Hostis, 2025).

The introduction of multi-banking and the establishment of a national electronic identity (e-ID) (Swiss Confederation, 2025) pursues the goal of simplifying authentication and enabling secure, interoperable financial services across institutions and sectors. As trusted custodians of sensitive financial data, Swiss banks are well positioned to play a role in this emerging identity ecosystem. Beyond traditional intermediation, they can act as verified issuers and validators of electronic identities and digital documents, leveraging their reputation, regulatory compliance, and security infrastructure. By expanding into identity and trust services, such as e-signature solutions, credential verification, and secure document exchange,

banks can open up new business fields that reinforce their role as trusted intermediaries in an increasingly digital environment.

Together with regulatory and technological enablers, these trends position the DXP as the secure gateway connecting banks, customers, employees, and partners within an increasingly connected digital ecosystem. Against this background, the digital experience platform in the baseline scenario is assessed in relation to the key requirements for future financial IT architectures and infrastructures:

- **Functionality:** The digital experience platform serves as the central orchestration layer for all customer interfaces, including mobile, web, social, marketplace, and Embedded Finance channels. It enables personalisation, omnichannel journeys, and coordinated customer interaction management, ensuring a consistent experience across touchpoints.

- **Modularity & flexibility:** Architecturally, the DXP is built on APIs, microservices, and a headless design that allow rapid onboarding of new channels and services. Loose coupling between presentation, logic, and data layers enables banks to extend or modify their digital front ends without disrupting underlying systems.

- **Data orientation & sovereignty:** The platform is inherently data-driven, leveraging customer analytics, recommender engines, and AI to deliver personalised, context-aware experiences. Achieving this requires consistent, real-time data flows from core banking systems and ecosystem partners, thereby establishing a single customer view. Data governance and interoperability play a crucial role in ensuring accuracy, compliance, and auditability across all connected systems.

In summary, the digital experience platform represents the customer- and employee-facing evolution of the financial IT landscape. Within the baseline scenario, it acts as the intelligent orchestration layer that personalises, automates, and enhances human interaction beyond traditional banking boundaries, turning the bank from a service provider into an integrated part of the customer's digital ecosystem.

## 4.4. Security Suite

Within the baseline scenario, the security suite constitutes a critical and foundational layer of the banking IT architecture, designed to safeguard sensitive data, preserve system integrity, and ensure resilience against internal and external threats. Rather than being limited to perimeter defence, the modern security suite operates as a distributed, adaptive system that protects data, applications, and infrastructure across hybrid and multicloud environments. Its evolution reflects a fundamental shift from static, compliance-driven security to continuous intelligence-based risk management.

Within Swiss banking, this transformation is strongly influenced by regulatory expectations around operational resilience, data protection, and management of third-party risks (FINMA, 2022). Security suites are increasingly embedded within enterprise architectures as orchestrators of trust and compliance, ensuring that every data flow, transaction, and API connection adheres to policy-defined risk thresholds. In this context, the suite acts as both a technical enabler and a governance instrument, linking cybersecurity with regulatory assurance and business continuity.

The baseline trajectory envisions an evolutionary expansion of the security layer along three dimensions: (1) deeper integration of zero-trust principles across all domains; (2) increased automation of detection and response through AI and behavioural analytics; and (3) stronger alignment with resilience and recovery frameworks that extend across institutions and providers (Morrison, 2025). As a result, the security suite no longer functions as a standalone system but as a pervasive, adaptive layer embedded within every architectural component, from the business platform to the decoupling and digital experience layers.

In the following, the security suite is assessed against the key requirements for future financial IT architectures and infrastructures:

- **Functionality:** The security suite consolidates core security domains, including identity and access management (IAM), privileged access control, encryption, key management, intrusion detection, and endpoint protection. It coordinates authentication and authorisation across internal systems, partners, and customers, supporting consistent pol-

icy enforcement and compliance reporting. Integrated audit and compliance modules ensure traceability of security events and facilitate adherence to regulatory standards such as FINMA requirements and ISO 27001. Advanced functions include continuous monitoring, integration of threat intelligence, and automated incident response.

- **Security, compliance & resilience:** This dimension represents the security suite's primary purpose. By implementing zero-trust principles, verifying every user, device, and connection, the platform enforces least-privilege access and continuous validation (Daah, Qureshi, & Awan, 2023). Built-in resilience mechanisms such as micro-segmentation, failover orchestration, and immutable backups ensure operational continuity.

- **Modularity & flexibility:** The security suite follows a service-oriented design, allowing independent deployment of components such as IAM, threat analytics, or encryption services. APIs and policy-as-code frameworks facilitate interoperability across core, middleware, and front-end systems. This modularity supports incremental adoption and integration into evolving multi-cloud and Open Finance environments.

- **Data orientation & sovereignty:** Security analytics increasingly rely on real-time telemetry and data correlation to detect anomalies and assess risks. Data sovereignty remains critical, as sensitive logs, credentials, and transaction records must remain within Swiss or jurisdictionally approved boundaries.

Overall, the security suite forms the foundational trust layer of the baseline architecture. It transforms cybersecurity from a defensive cost centre into a proactive enabler of digital trust and regulatory assurance.

## 4.5. Data Factory

In the baseline scenario, the data factory serves as the technological backbone of data-driven banking. It consolidates the collection, integration, and transformation of structured and unstructured data within the institution and its ecosystem, enabling analytics, automation, and AI applications.

Operating in hybrid environments, the platform combines on-premises and cloud components to balance regulatory control and scalability (see, e.g., Susnjara and Smalley (online) on hybrid cloud architectures). Legacy systems are gradually integrated via standardised APIs, while new modules are developed as cloud-native services. Architecturally, the platform follows a layered "zone" model, from raw to trusted to business-ready data, ensuring governance, flexibility, and modular growth.[1] Over time, institutions are expected to embrace lakehouse or data fabric architectures. A lakehouse combines the scalability of data lakes with transactional and BI capabilities, while a data fabric weaves together distributed nodes across on-premises and cloud, abstracting complexity and enabling ubiquitous data access for example across hybrid and multi-cloud environments (Sarkar, online).

A key trend in the baseline scenario is the shift from batch to real-time data flows. Streaming architectures and change-data-capture (CDC) mechanisms allow only deltas (i.e., inserts, updates, and deletions) to be captured and propagated efficiently, enabling low-latency analytics (Abdelaty, 2025) for fraud detection, payments monitoring, and personalised services. Complemented by robust metadata and data lineage frameworks, every transformation and data path becomes traceable, ensuring auditability, regulatory compliance (e.g., BCBS 239), and institutional trust (Collibra, 2025). Together, these elements make the data factory not just a processing engine, but the enabler of scalable, governed, real-time analytics and innovation across the financial value chain.

The data factory is in the baseline scenario assessed against key requirements for future financial IT architectures:

- **Economic efficiency:** Shared infrastructure, reusable data pipelines, and consumption-based operating models reduce redundancy and optimise resource use. Automation in data quality management and pipeline orchestration further increases efficiency and lowers operational costs. In addition, systematic data cleansing within banks simplifies future system integration or migration efforts and thereby helps to prevent additional costs over time.

[1] Such zoning strategies are increasingly applied in financial data architectures to balance security, regulatory compliance, and analytics capabilities (Talati, 2025).

- **Security, compliance & resilience:** The consolidation of sensitive data across systems and partners heightens the need for strong protection mechanisms. Encryption, granular access control, and continuous monitoring safeguard integrity and confidentiality, while metadata and lineage ensure transparency and auditability. Embedded resilience measures such as redundancy and failover processes maintain trust and operational continuity even under adverse conditions.

- **Modularity & flexibility:** Built on loosely coupled pipelines and standardised APIs, the data factory supports incremental expansion and selective replacement of components. New data domains or analytics modules can be added without affecting core operations. This design principle enables continuous evolution of the data landscape, ensuring scalability and resilience amid changing regulatory and technological environments.

- **Data orientation & sovereignty:** By treating data as a governed and reusable asset, the data factory ensures consistent, high-quality datasets across systems. Clear ownership, purpose limitation, and consent management preserve data sovereignty, especially across hybrid and multi-cloud environments, while enabling secure collaboration within Open Finance ecosystems.

In summary, the data factory in the baseline scenario forms the analytical backbone of the financial IT landscape. It connects legacy and modern systems, transforms raw information into actionable insights, and enables institutions to leverage their data assets efficiently while ensuring trust, compliance, and governance across the organisation.

## 4.6. Multi-Cloud Platform

From the perspective of the baseline scenario, multi-cloud adoption marks a decisive step toward more resilient and sovereign financial IT architectures, balancing regulatory and operational priorities with innovation. Multi-cloud platforms provide the strategic foundation for deploying workloads, data, and digital services across several providers and technologies. They enable financial institutions to meet regulatory expectations for sovereignty, portability, and concentration risk management while simultaneously pursuing flexibility, performance, and cost efficiency. Rather than depending on a single hyperscaler, banks distribute workloads across multiple clouds, hybrid environments, and on-premises systems to ensure agility, mitigate vendor lock-in, and maintain compliance (Basel Committee on Banking Supervision, 2024).

From an architectural and infrastructure perspective, multi-cloud strategies are in the baseline scenario assessed against key requirements for future financial IT architectures:

- **Economic efficiency:** The multi-cloud platform allows dynamic workload distribution and cost optimisation through provider benchmarking and workload scheduling. However, financial institutions must ensure consistent governance and compliance across jurisdictions. Initiatives such as the EU Data Act demand explicit switching rights and prohibit undue exit barriers (Lindberg & Tegnvallius Boklund, online), reinforcing the need for portable architectures, transparent vendor contracts, and appropriate vendor management.

- **Security, compliance & resilience:** Regulators increasingly require institutions to demonstrate cloud portability, exit strategies, and mitigation of concentration risks. As multi-cloud environments become more complex, maintaining consistent identity and access management across providers has emerged as a core challenge for financial institutions. Harmonised security policies and zero-trust frameworks are essential to mitigate compliance and resilience risks in the future (Alexander, 2025; Olden, 2025). A multi-cloud setup enhances resilience through cross-provider redundancy, failover capabilities, and geographic diversification. Sovereign cloud architectures, local key custody, and privacy-preserving analytics (e.g., homomorphic encryption or federated learning) ensure that risk management and compliance can coexist with innovation.

- **Modularity & flexibility:** Workloads are now increasingly deployed in containerised, cloud-agnostic environments that enable seamless portability across providers. As Pacheco (2024) emphasises, cloud-agnostic design reduces depen-

dency on individual providers and fosters greater flexibility across environments. Building on this foundation, many institutions are establishing multi-cloud control planes to coordinate policies, monitoring, and deployment pipelines across heterogeneous infrastructures. This approach also enables the use of the latest hardware architectures, such as graphics processing units (GPUs) or, in the future, quantum computing. This aspect is particularly significant as AI workloads continue to drive demand for high-performance computing resources.

Overall, the multi-cloud platform represents the evolution from isolated cloud adoption to orchestrated and interoperable cloud ecosystems. It forms the technological foundation for resilience and sovereignty in digital finance, enabling banks to balance innovation and compliance while reducing systemic dependence on single providers.

## 4.7. IT Governance, Management, and Development

Gartner (2025) notes that "the decentralized, self-service nature of cloud computing has taken the power of computing out of IT's hands and distributed it to the business units. IT is now in a precarious position, balancing its responsibility to protect the organization from risk with ensuring that business units can maintain their agility and freedom to innovate". Within the baseline scenario, IT governance, management, and development practices evolve precisely along this tension, aiming to align protection, compliance, and innovation. Traditional waterfall or silo-based oversight is increasingly replaced by adaptive governance structures that link strategic IT management with agile, DevSecOps-driven execution.

In the financial sector, this shift is not optional but a strategic necessity. Increasing regulatory complexity and accelerating digital transformation require governance frameworks that balance control with speed and autonomy. As financial institutions digitise core processes, continuous integration and delivery (CI/CD) pipelines have become central to ensuring both innovation and compliance (Fitsak & Neville, 2025). Governance bodies continue to define strategic guardrails, clarifying decision rights, escalation paths, and accountability structures, while day-to-day control increasingly shifts toward agile delivery and development operations. Metrics are moving beyond static compliance checkboxes toward continuous, data-driven KPIs. Modern DevSecOps metrics, including deployment frequency, change failure rate, and mean time to recovery, offer a combined view of agility, stability, and risk (Moustakis, 2025). Over time, policy-driven modular architectures and automated governance tools allow financial institutions to reduce friction between regulation and innovation, ensuring that compliance becomes part of development, not an obstacle.

The domain IT governance, management, and development is assessed against three main requirements:

- **Economic efficiency:** As financial institutions seek to shorten delivery timelines and optimise resource use, automation and integrated DevSecOps frameworks have become essential enablers of efficient and controlled software development. Embedding "security-as-code" within CI/CD pipelines, as Jesis (2024) emphasises, enables consistent and automated enforcement of security and compliance policies while reducing manual overhead. Consequently, DevOps and DevSecOps have become key enablers for improving economic efficiency, as they streamline release processes, reduce operational costs, and ensure governance integrity through built-in automation (PreEmptive, online).

- **Security, compliance & resilience:** Rising regulatory complexity and operational interdependence require that security and compliance become integral parts of IT governance and development practices rather than afterthoughts. This shift increases the importance of embedding control mechanisms directly into development pipelines. As GitLab Inc. (online) notes, incorporating automated vulnerability scanning, policy enforcement, and compliance validation within DevSecOps frameworks allows institutions to detect and remediate risks much faster. Governance frameworks must therefore evolve toward proactive resilience management, emphasising continuous monitoring, clear accountability, and integrated risk oversight throughout the development and delivery lifecycle.

- **Modularity & flexibility:** As both organisational demands and regulatory frameworks become more dynamic, institutions must adopt governance and

development models that enable continuous, modular adaptation rather than periodic large-scale transformation. Modular structures allow functions and components to be developed, tested, and deployed independently, improving adaptability and reducing systemic risk. This flexibility strengthens institutional responsiveness to technological and regulatory change.

In essence, IT governance under the baseline scenario shifts from static oversight to dynamic orchestration. Automation and modularity enable financial institutions to uphold regulatory integrity while fostering innovation capacity, creating a governance model that supports both operational stability and strategic adaptability.

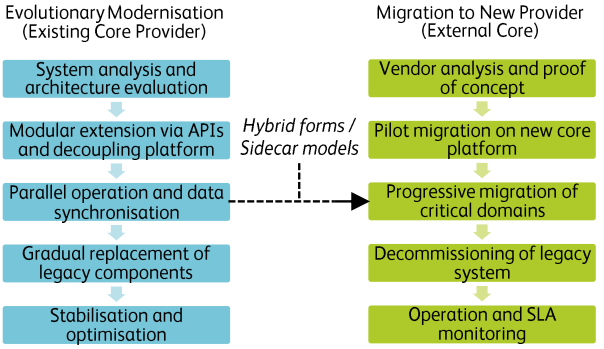


Figure 4.1: Roadmap: Evolutionary modernisation vs. migration to a new provider

## 4.8. Roadmap

As highlighted in the Swisscom Core Banking Radar, many institutions are extending their existing systems by adding modular components, open interfaces, and cloud compatibility instead of replacing them entirely (Tunçer et al., 2025). This evolutionary path reflects a pragmatic response to the complexity and risk of large-scale system replacements. Incremental transformation allows banks to modernise critical components step by step, maintaining operational continuity and reducing implementation risk. However, this gradual approach can also prolong technical debt and limit the speed of innovation.

Against this backdrop, the transformation towards future-ready business platforms requires a structured and evolutionary roadmap that balances innovation with operational stability. In the baseline scenario, most Swiss banks pursue this gradual transformation rather than embarking on disruptive, large-scale migrations, a reflection of both regulatory prudence and the long-term investment cycles typical of the Swiss banking industry. The roadmap thus outlines how institutions can modernise their IT architectures in a controlled manner while progressively enabling new business models and technological capabilities. Within the scope of this study, the roadmap highlights the core banking domain as a key reference point for understanding the broader shift toward platform-based financial architectures. Its perspective remains centred on the architectural and provider layer, while acknowledging that full digital transformation extends beyond the core.

Figure 4.1 illustrates how Swiss institutions can follow two primary transformation trajectories: an **evolutionary modernisation path** with the existing provider and a **migration path** to a new core banking provider. Both paths share a similar sequencing of phases, ranging from architectural assessment to stabilisation, but differ fundamentally in scope, speed, and organisational impact.

In the evolutionary roadmap (left side of the figure), banks progressively modernise their existing cores through modular extensions, API gateways, and the gradual build-up of a decoupling platform that separates legacy systems from new digital services. This enables the coexistence of legacy and new environments through parallel operation and continuous data synchronisation, allowing innovation without endangering daily operations. Over time, legacy components are hollowed out, and the overall system architecture becomes more modular and interoperable. This evolutionary transition is followed by a new phase of continuous stabilisation and optimisation, and is particularly suited to institutions with complex, deeply integrated infrastructures and strong dependencies on established providers. Such an approach is often favoured by banks with extensive legacy systems, a cautious risk culture that seeks to avoid large-scale migrations, and cost considerations that prioritise incremental modernisation over full replacement.

In the migration roadmap (right side of the figure), institutions analyse vendors and feasibility. Consequently, they choose to transition to a new, cloud-native core plat-

form (neo core banking platform). This process typically begins with pilot modules or selected customer segments and proceeds through staged migration waves until the legacy environment is eventually decommissioned. In the resulting new setup, institutions can focus on monitoring operations and service fulfilment. While this route offers a cleaner technological foundation and greater long-term agility, it requires significant investment, extensive migration planning, and robust data governance.

Between these two extremes, hybrid forms, often referred to as "sidecar" models, have emerged as a conceptual approach explored by several institutions seeking to balance innovation with operational continuity. These combine elements of both strategies. Banks deploy a separate, cloud-based stack for new products or customer groups and maintain their existing core for stable operations. Over time, such platforms can be expanded to gradually replace legacy components. In this sense, they resemble a "greenfield" initiative, an entirely new technology stack created as part of a broader business model innovation rather than a conventional migration (Rhyner, 2023a).

Overall, the roadmap highlights that there is no single blueprint or established best practice for the transformation of core systems. Each institution must balance innovation ambition, risk tolerance, and resource capacity. What unites all approaches, however, is the strategic imperative to move toward modular, data-driven, and interoperable architectures, ensuring that Swiss banking IT remains resilient, compliant, and innovation-ready in the coming decade.

# 5. Alternative Scenarios

In addition to the baseline scenario in Chapter 4, three exemplary disruptive future scenarios are examined in more detail to illustrate potential technological and structural developments in the financial system. The three examples are a financial system without banks (Section 5.1), a fully automated bank without human staff (Section 5.2), and a centralised transaction bank (Section 5.3). None of these futures is expected to be realised in its pure form, yet each highlights distinct opportunities, challenges, and design choices. Moreover, individual elements from these scenarios may be integrated into the baseline trajectory, shaping the future architecture of finance.

In addition to the three technology-oriented examples, other scenarios are conceivable. One example is a self-sufficient bank that strives for complete independence and control. Such a self-sufficient institution could address geopolitical, technological, and other systemic risks by maintaining a highly autonomous infrastructure with minimal interfaces and external dependencies. However, since this scenario, and also others, involves relatively little technology, it is not further considered in this technology-oriented report.

## 5.1. Bank-less Financial System

DLT represents a potential foundation for a bank-less financial system as it provides a decentralised, transparent, and tamper-resistant infrastructure. By design, DLT enables transactions to be validated and recorded without the need for central intermediaries, ensuring trust through consensus mechanisms rather than institutional oversight. These characteristics make it a plausible technological basis for imagining a financial system in which traditional banks no longer play a central role.

The basis for a bank-free financial system could consist not only of DLT but also of an ecosystem of FinTech and BigTech companies that provide the relevant services and processes. In what follows, however, the analysis focuses on a DLT-based financial system that operates without intermediaries. In doing so, we focus on technical and economic factors and leave regulatory factors aside.

Building on this technological foundation, decentralised finance (DeFi) can be seen as the practical manifestation of such a system. DeFi represents a new financial ecosystem built on blockchain networks, where decentralised financial services can operate without banks or centralised institutions (Schär, 2021). At its core, DeFi relies on smart contracts, which are self-executing programs that automatically enforce rules when certain conditions are met (Ethereum Foundation, 2025). This allows individuals or corporates to pay, lend, or borrow funds, and trade crypto assets directly (FINMA, 2021), with every transaction transparently recorded on the blockchain.

Technically, DeFi functions through decentralised applications, or dApps (Schär, 2021), which connect to users' wallets. Users interact with these dApps by depositing crypto assets or initiating transfers, after which smart contracts automatically execute transactions in real time, including clearing, settlement, and interest payments.

DeFi services already cover a wide spectrum, ranging from lending and borrowing platforms to staking mechanisms, yield farming strategies, decentralised exchanges, and flash loans. The scale of the ecosystem has expanded significantly in recent years. As of October 2025, the total value locked (TVL) metric, measuring the total amount of assets deposited in DeFi protocols, exceeded USD 170 billion (DefiLlama, online). This indicates not only that DeFi has moved beyond experimental applications, but also that it has grown into a sizeable and increasingly relevant component of the broader crypto asset landscape, suggesting how such technologies could one day underpin a bank-less financial system.

The following points outline how a bank-less financial system based on DeFi might align with the five key requirements of future financial infrastructures:

- **Functionality:** Such a system would aim to replicate the essential functions of a bank, including payments, savings, loans, and investments, while also enabling new types of financial products. However, not all services could be mirrored one-to-one, since the underlying mechanisms differ. While traditional banking relies on centralised credit assessment, guarantees, and regulatory oversight, a decentralised system would operate on collateralisation, algorithmic rules, and decentralised gover-

nance. Certain services may be more difficult to realise in this setup, though this might change as decentralised identity, reputation systems, and governance mechanisms evolve.

- **Economic efficiency:** By eliminating intermediaries and automating processes through smart contracts, the system could, in theory, reduce costs and increase efficiency. At the same time, efficiency would depend on the scalability of the underlying technology, and hidden costs such as network fees or user complexity could remain.

- **Security, compliance & resilience:** Trust would shift from regulated institutions to technology. Blockchains, in theory, provide robustness and transparency, but smart contract vulnerabilities, oracle dependencies, and governance risks could threaten stability. Without institutional and regulatory protections, resilience would have to be achieved through technical safeguards, auditing, and decentralised risk management mechanisms.

- **Modularity & flexibility:** A DLT-based bank-less system would be highly modular, with dApps serving as the building blocks of financial services. These dApps could be combined and layered to enable rapid product innovation and adaptation. This flexibility, however, could also amplify systemic risks, as the failure of one application or protocol might propagate through interconnected services.

- **Data orientation & sovereignty:** Transactions would be publicly visible on the blockchain, and users would retain direct control of their assets through private keys. This enhances sovereignty and transparency but also shifts responsibility for security, compliance, and key management fully to the individual.

In summary, a bank-less financial system based on DLT is conceivable as a thought experiment in which decentralised technologies replace many functions traditionally performed by banks. Such a system could provide transparency, innovation, and new forms of financial interaction, but would also impose high demands on the knowledge, responsibility, and risk management of its participants. The absence of institutional advisory and protection mechanisms raises the question of whether complementary technologies, such as AI, might eventually help individuals navigate and manage this decentralised environment.

## 5.2. Human-less Bank

(Agentic) AI could serve as a potential foundation for a human-less bank, where all operations are fully automated and no human staff are required. Agentic AI involves autonomous agents that execute multi-step workflows, communicate with APIs, and make decisions dynamically based on evolving input and adapting goals (Thürig, Cruz, & Xiao, 2025). One can imagine a financial institution that runs entirely on algorithms and digital interfaces, providing clients with seamless, 24/7 access to services without the involvement of human employees (Ghose et al., 2025).

In such a system, account opening and management become instantaneous. Customers could verify their identity via biometric authentication and immediately begin depositing funds, initiating transfers, or setting up standing orders. Payment services such as domestic transfers, direct debits, and international transactions would be executed automatically, with AI constantly monitoring transactions for irregularities and preventing fraud (World Economic Forum, 2025a). For more complex services like loans and investments, algorithms would provide tailored advice, risk assessments, and real-time approval decisions based on each client's profile. Customer support would be delivered through AI-driven assistants, capable of offering context-aware answers to queries and personalised guidance (Barbey et al., 2025).

The following points outline how a human-less bank might align with the five key requirements of future financial infrastructures:

- **Functionality:** Such a system would cover the core operational and advisory functions of a bank, including payments, savings, loans, and investments. Standardised processes could be fully automated, while more strategic or creative functions, such as process design or long-term strategic planning, might remain challenging to replicate through algorithms alone.

- **Economic efficiency:** Automation would reduce the need for human resources and enable cost-

efficient scaling. Services could be delivered instantly and at lower marginal cost. However, initial investments in infrastructure and AI models would be significant, and adoption may depend on user trust and regulatory approval.

- **Security, compliance & resilience:** AI-driven monitoring could enhance fraud detection and cybersecurity, while automated protocols ensure consistency and reliability. At the same time, reliance on algorithms introduces risks such as systemic errors, model biases, or vulnerabilities to cyberattacks, which could undermine resilience.

- **Modularity & flexibility:** A human-less bank would likely focus on standardised, repeatable processes, which can be modularised but not as flexibly recombined as in human-driven systems. While automation ensures efficiency, it may limit adaptability to unique customer needs or unforeseen conditions.

- **Data orientation & sovereignty:** Such a bank would be highly data-driven, relying on continuous analysis of personal and financial data. While this could improve personalisation, it also raises concerns about user sovereignty, as customers may have limited control over how their data is collected, processed, and applied.

In summary, a human-less bank illustrates a possible future where AI technologies replace most operational and advisory functions traditionally performed by people. This could create a fast, efficient, and transparent system, but also one where trust depends on algorithms rather than personal interaction. The success of such a model would ultimately depend on user acceptance, regulatory frameworks, and the ability of AI systems to demonstrate accountability and resilience.

## 5.3. Large-scale Transaction Bank

A large-scale transaction bank represents a possible future in which the financial industry consolidates core operational components into centralised, shared platforms. The idea is well researched (see, e.g., Riese (2006)) and is rooted in industrial logic, whereby economies of scale are created when components of a business model can be centralised across multiple institutions. The concept of a component-based company should therefore be applied to an entire industry (e.g., "Einheitskasse" in health insurance) or a network of institutions. Main areas of business in retail banking are payment services, deposit services, investment services, and lending services, each of which consists of various components. In the investment area in Switzerland, a centralised player is already in place, with SIX covering components such as exchange, clearing, settlement, and securities depository. Payment transactions, as another example, are a commodity service that does not generate attractive margins for a bank (Kaib, 2008), but must still be offered. However, the corresponding value chain remains more fragmented across smaller transaction-processing banks, major institutions, and specialised service bureaus.

This scenario describes a large-scale transaction bank for payment transactions as a centralised institution that would be responsible for processing, managing, and recording payments in a network of banks. Its primary role would be to consolidate domestic payments, settlement, and cash management operations into a single, unified ledger. Existing payment infrastructures could still be integrated for clearing outside the network and for cross-border payments. By replacing multiple decentralised solutions with a unified platform, the transaction bank would provide a holistic view of liquidity positions, counterparty exposures, and financial flows.

The following points outline how a large-scale transaction bank could align with the five key requirements of future financial infrastructures:

- **Functionality:** A transaction bank would provide essential backbone services for the processing of payments and settlements across participating banks. It would standardise core components such as clearing, reconciliation, settlement, and liquidity management, ensuring uniform processes and consistent operational quality across the network. The platform would support integration with existing infrastructures for cross-border and interbank payments. As the model matures, additional value chain components such as lending or securities operations could migrate to similar shared platforms.

- **Economic efficiency:** Such a transaction bank directly addresses the challenge of inefficiencies and rising costs within individual banks' technology stacks (itopia, 2025). These costs stem from heterogeneous products, complex processes, redundant IT environments, numerous digitalisation projects,

and the maintenance of legacy systems. The potential for substantial cost savings lies in standardisation, automation, and increased scalability. A centralised ledger for payment transactions would standardise processes, reduce manual intervention, and enhance straight-through processing capabilities. Implementing such a modern processing platform for an individual bank on its own is very costly. However, if costs were shared among several banks, the barrier to entry would be significantly lower. As a shared infrastructure, the transaction bank would enable economies of scale, reduce duplication, and lower transaction costs, while supporting joint investments in new technologies. This consolidation would not limit banks' ability to differentiate themselves, as payment processing remains largely invisible to end customers.

- **Security, compliance & resilience:** A centralised transaction bank would deliver high operational reliability, governed by stringent security and compliance standards. As a technological backbone, it would have to operate a scalable, zero-downtime ledger platform using cloud-based technologies that ensure security, availability, and resilience. The model would strengthen governance by providing unified visibility into liquidity, risk exposure, and settlement operations. However, centralisation also introduces concentration risk, as system failure, cyberattack, or disruption could impact all participating banks simultaneously. Consequently, redundancy mechanisms, strong regulatory oversight, and independent auditing would be essential to maintain system stability.

- **Modularity & flexibility:** The transaction bank would be designed as a modular platform offering standardised interfaces and API-based integration. This structure would allow participating banks to connect seamlessly, automate processes, and adapt more easily to regulatory or market changes. It would also simplify the implementation of new requirements and support integration with emerging infrastructures such as instant payments, Open Banking, and central bank digital currencies (CBDCs). In this setup, traditional banks could connect to the APIs of the decoupling platform of each component supplier and focus on differentiating their customer experience layers, rather than maintaining redundant back-end systems. However, the high level of standardisation may limit flexibility for individual banks when designing tailored products or services. Success would therefore depend on balancing standardisation with customisation options at the edges of the platform.

- **Data orientation & sovereignty:** A shared ledger would create a single source of truth for payments and liquidity data, enabling consistent reporting, enhanced transparency, and improved risk management across the network. Centralised data structures would also facilitate better governance and auditability. However, this model raises important questions regarding data ownership, confidentiality, and access rights. Robust data governance frameworks, clear contractual arrangements, and adherence to national data protection regulations would be essential to ensure trust and maintain compliance.

Overall, the technical feasibility of such a configuration is likely given, but its realisation would depend on the intensity of competition, regulatory acceptance, and the willingness of institutions to reassess existing decentralised structures. Implementation would therefore require not only technological readiness but also strategic coordination and industry-wide collaboration.

In summary, a large-scale transaction bank represents a scenario in which efficiency, consolidation, and standardisation reshape the operational foundations of the banking sector. It promises lower costs, enhanced process automation, and improved oversight through unified visibility into liquidity and risk exposure. Moreover, it aligns banks with emerging infrastructures such as instant payments, Open Banking, and CBDCs, while enabling more efficient implementation of regulatory requirements. Similar to payments, other components of the banking value chain, such as lending, could also shift to scalable, specialised platform providers. In such a structure, traditional banks would connect to component suppliers via APIs and focus on differentiated customer experiences. Ultimately, this scenario illustrates one possible pathway toward further market consolidation and industrialisation within the Swiss financial sector.

# 6. Conclusion and Outlook

This chapter summarises the report in the form of a set of hypotheses about future IT architectures and infrastructures.

**Future IT architectures and infrastructures must satisfy diverse and sometimes conflicting requirements.** Security, compliance, and resilience will remain non-negotiable priorities while, from a business perspective, functionality at the lowest possible cost will continue to dominate decision-making. To meet these needs, financial IT systems must become modular, data-centric, and flexible, capable of integrating new technologies without jeopardising operational integrity or regulatory compliance.

**The evolution of banks' IT architectures and infrastructures is expected to remain predominantly incremental rather than revolutionary.** The business platform, or core banking platform, will continue to serve as the central element of this transformation. But in the long term, the question arises not only of innovative capability but also of whether today's core system architecture allows for a competitive cost base. Two strategic pathways can be distinguished: first, the further development of existing platforms in close collaboration with providers and other partner banks; and second, the migration to a new, often cloud-native, neo core banking platform. In practice, most institutions are likely to pursue the first path, enhancing their current systems instead of initiating large-scale replacements. However, larger banks or banking groups may complement their existing infrastructures with hybrid "sidecar" solutions or launch greenfield initiatives to support innovative business models. These developments open significant opportunities for neo core banking providers and FinTech companies offering specialised modular components.

**The decoupling platform will play a pivotal role in an evolutionary transformation scenario.** In the baseline trajectory, the decoupling platform serves as a strategic integration layer that interconnects core systems, internal applications, and external ecosystems. This architecture enables banks to gradually expand and modularise their existing infrastructures. The evolution typically starts with decoupling internal domains, then proceeds to the controlled opening of interfaces to partners within the framework of Open Finance, and ultimately extends to cross-institutional integration. In this way, the decoupling platform forms the architectural backbone for modularity, interoperability, and secure openness, allowing institutions to innovate, collaborate, and evolve without compromising the stability of their operational core. However, it is essential to bear in mind that the decoupling platform is exposed on the internet and therefore subject to the highest cyber resilience requirements.

**Multi-cloud platforms will form the foundation of future IT architectures.** Multi-cloud platforms provide the strategic basis for deploying workloads, data, and digital services across multiple providers and technologies, while seamlessly also integrating on-premises or edge environments. This approach enables institutions to leverage cutting-edge hardware architectures, thereby enhancing computational performance and scalability. Such capabilities will be particularly relevant in light of the growing processing demands of AI and other data-intensive applications.

**Data and AI capabilities will increasingly determine the competitiveness of financial institutions.** The data factory will become the analytical core of future architectures, enabling real-time processing, regulatory traceability, and data-driven decision-making. AI will transform both customer interaction and operational efficiency, but its integration requires robust governance, traceable data lineage, and ethical oversight. The data factory also serves applications that do not require real-time data from the core banking system. This reduces the load on the business platform and mitigates performance bottlenecks.

**Disruptive architectures and infrastructures are theoretically feasible.** Concepts such as a financial system without banks, fully automated banks without human involvement, or a centralised national transaction bank are technically possible with today's or near-future technologies such as AI or DLT. Such disruptive architectures could offer efficiency gains as well as new forms of value creation and competition. However, they would also entail substantial risks and trade-offs compared to the current system. The evolutionary path outlined in this report therefore remains the more plausible trajectory. Nevertheless, individual elements of these disruptive models may gradually find their way into evolutionary developments of the financial system.

# Authors

This condensed study was prepared in collaboration with the following individuals, who contributed to its content (in alphabetical order):


## Authors HSLU

**Prof. Dr. Thomas Ankenbrand**
Head Competence Center Investments

**Dr. Denis Bieri**
Lecturer

**Joël Ettlin**
Research Associate

**Dr. Thomas Fischer**
Lecturer

## Guest Author in Addition to the Authors from the HSLU

**Urs Rhyner**
Head InventxLab
Inventx AG


We would also like to thank the research partners of this study, namely Canton of Zug, Finnova, Finstar, Inventx, SFTI / Swiss Fintech Innovations, SIX, and Zürcher Kantonalbank, for their monetary and content-related support, including discussions and document reviews.

## Contact

For more information about this study, please contact us at:

**Thomas Ankenbrand**
Lucerne University of Applied Sciences and Arts
thomas.ankenbrand@hslu.ch

# References


Abdelaty, K. (2025). *What is Change Data Capture (CDC)? A Beginner's Guide.* Retrieved 15/10/2025, from https://www.datacamp.com/blog/change-data-capture

Alexander, N. (2025). *Strategies to Secure Multi-Cloud Environments in Financial Services.* Retrieved 16/10/2025, from https://www.bobsguide.com/strategies-to-secure-multi-cloud-environments-in-financial-services/

Ankenbrand, T., Bieri, D., & Gattlen, A. (2025). *IFZ FinTech Study 2025. An Overview of Swiss and Liechtenstein FinTech.* Retrieved 03/09/2025, from https://hub.hslu.ch/retailbanking/download/ifz-fintech-study/

Avaloq. (2019). *Successful Introduction of Avaloq Platform at Raiffeisen.* Retrieved 29/10/2025, from https://www.avaloq.com/insights/press-releases/successful-introduction-of-avaloq-platform-at-raiffeisen

Barbey, R., Grimond, L., Maguire, A., Maida, D., Mishra, Y., Ramachandran, S., … Scotti, A. (2025). *Tech in Banking 2025: Transformation Starts with Smarter Tech Investment. Boston Consulting Group (BCG).* Retrieved 13/10/2025, from https://www.bcg.com/publications/2025/tech-banking-transformation-starts-with-smarter-tech-investment

Basel Committee on Banking Supervision. (2021). *Revisions to the Principles for the Sound Management of Operational Risk.* Retrieved 29/10/2025, from https://www.bis.org/bcbs/publ/d515.pdf

Basel Committee on Banking Supervision. (2024). *Digitalisation of Finance.* Bank for International Settlements. Retrieved 23/09/2025, from https://www.bis.org/bcbs/publ/d575.pdf

Berchtold, N., Amrein, S., & Dietrich, A. (2025). *Marketplace Lending Report Switzerland 2025.* Retrieved 04/11/2025, from https://hub.hslu.ch/retailbanking/download/marketplace-lending-report-switzerland/

Blattmann, U., & Buschor, F. (2023). *Zukunft der Kernbankensysteme – erste Erkenntnisse der Studie.* IFZ Retail Banking Blog, Hochschule Luzern. Retrieved 06/11/2025, from https://hub.hslu.ch/retailbanking/zukunft-der-kernbankensysteme-erste-erkenntnisse-der-studie/

Blattmann, U., Buschor, F., & Ettlin, J. (2023). *IFZ Studie Zukunft der Kernbanksysteme.* Retrieved 04/11/2025, from https://blog.hslu.ch/bankingservices/files/2023/06/IFZ-Studie-Zukunft-der-Kernbankensysteme_v2.pdf

Blattmann, U., Buschor, F., & Ettlin, J. (2024). *IFZ Studie Bank-IT und Sourcing 2024.* Retrieved 04/11/2025, from https://drive.switch.ch/index.php/s/HHAQF6fXrK1936I

Blattmann, U., Fischer, T., & Ettlin, J. (2025). *IFZ Studie Bank-IT und Sourcing 2025.* Retrieved 04/11/2025, from https://drive.switch.ch/index.php/s/hWr90YJy89we8fF

Collibra. (2025). *Four Ways Data Lineage Powers BCBS 239 Compliance.* Retrieved 15/10/2025, from https://www.collibra.com/blog/four-ways-data-lineage-powers-bcbs-239-compliance

Daah, C., Qureshi, A., & Awan, I. (2023). *Zero Trust Model Implementation Considerations in Financial Institutions: A Proposed Framework.* In *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud).* Retrieved 14/10/2025, from https://www.researchgate.net/publication/377796472_Zero_Trust_Model_Implementation_Considerations_in_Financial_Institutions_A_Proposed_Framework

Day, D. (2024). *Evaluating and Selecting Core Banking Systems: A Comprehensive Guide.* Retrieved 04/11/2025, from https://www.linkedin.com/pulse/evaluating-selecting-core-banking-systems-guide-douglas-day-ntttc/

Deb, S. (2023). *How Banks Are Using Middleware to Advance Innovation.* Retrieved 23/09/2025, from https://bankingjournal.aba.com/2023/02/how-banks-are-using-middleware-to-advance-innovation/

DECTA. (2025). *Digital Banking Customer Experience Trends 2025.* Retrieved 26/09/2025, from https://www.decta.com/company/media/digital-banking-customer-experience-trends-2025

DefiLlama. (online). *Total Value Locked in DeFi.* Retrieved 07/10/2025, from https://defillama.com/

Dietrich, A. (2025). *UBS key4 insights: Zwei Jahre Data Driven Banking im Praxistest.* IFZ Retail Banking Blog, Hochschule Luzern. Retrieved 04/11/2025, from https://hub.hslu.ch/retailbanking/ubs-key4-insights-zwei-jahre-data-driven-banking-im-praxistest/

Dietrich, A., & Amrein, S. (2024). *Wer hat das beliebteste Mobile Banking?* IFZ Retail Banking Blog, Hochschule Luzern. Retrieved 04/11/2025, from https://hub.hslu.ch/retailbanking/wer-hat-das-beliebteste-mobile-banking/

Ernst & Young. (2025). *EY Bankenbarometer 2025: Balance.* Retrieved 04/11/2025, from ey-bankenbarometer-2025.pdf

Ethereum Foundation. (2025). *Decentralized Finance (DeFi) — How DeFi Works.* Retrieved 07/10/2025, from https://ethereum.org/defi/#how-defi-works

European Central Bank. (2024). *Guide on Outsourcing Cloud Services to Cloud Service Providers.* Retrieved 29/10/2025, from https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603_draftguide.en.pdf

European Commission. (2025). *Loose Coupling.* Simpl Programme. Retrieved 04/11/2025, from https://simpl-programme.ec.europa.eu/book-page/loose-coupling

Eurostat (via Statista). (2024). *Anteil der Schweizer Bevölkerung, der das Internet für Online-Banking nutzt (2014–2023).* Statista. Retrieved 04/11/2025, from https://de.statista.com/statistik/daten/studie/431745/umfrage/nutzung-des-internets-fuer-online-banking-in-der-schweiz/

Federal Reserve. (2025). *Cybersecurity and Financial System Resilience Report.* Retrieved 04/11/2025, from https://www.federalreserve.gov/publications/files/cybersecurity-report-202507.pdf

FINMA. (2018). *Circular 2018/3 – Outsourcing: Banks and Insurance Companies.* Retrieved 29/08/2025, from https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf

FINMA. (2021). *Decentralized Finance (DeFi).* Retrieved 07/10/2025, from https://www.finma.ch/de/dokumentation/dossier/dossier-fintech/decentralized-finance-defi/

FINMA. (2022). *Circular 2023/1 – Operational Risks and Resilience – Banks.* Retrieved 25/09/2025, from https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf

FINMA. (2024). *FINMA Risk Monitor 2024: Principal Risks for the Financial Sector and Uncertainties Due to Geopolitical Tensions.* Retrieved 10/09/2025, from https://www.finma.ch/en/news/2024/11/20241118-mm-finma-risikomonitor-24/

Fischer, T. A., & Dibbern, J. (2024). *Strategic sourcing decisions: A Swiss bank responding to the dynamics of the core banking system market. Journal of Information Technology Teaching Cases*, *0*(0). Retrieved 04/11/2025, from https://journals.sagepub.com/doi/full/10.1177/20438869241280978

Fitsak, S., & Neville, M. (2025). *DevOps in Banking: The Complete Guide.* Retrieved 16/10/2025, from https://softjourn.com/insights/devops-in-banking

Gamma, M. (2021). *800 Millionen Migrationskosten und unzufriedene Bankkunden.* Retrieved 04/11/2025, from https://www.inside-it.ch/post/800-millionen-migrationskosten-und-unzufriedene-bankkunden-20210603

Gartner. (2025). *IT Governance: Adapt to Meet the Challenges of Cloud.* Retrieved 16/10/2025, from https://www.gartner.com/en/articles/it-governance

Gartner Peer Insights. (2025). *Digital Experience Platforms Reviews and Ratings.* Retrieved 04/11/2025, from https://www.gartner.com/reviews/market/digital-experience-platforms

Ghose, R., Bantandis, S., Master, K., Shah, R., Chahal, S., Sharma, P., & Zhai, C. (2025). *Agentic AI Finance & the 'Do It For Me' Economy.* Retrieved 04/11/2025, from https://www.citigroup.com/global/insights/agentic-ai

GitLab Inc. (online). *DevSecOps: The Key to Modern Security Resilience.* Retrieved 16/10/2025, from https://about.gitlab.com/the-source/security/devsecops-the-key-to-modern-security-resilience/

Hess, R. (2024). *"The key is combining trustworthiness with modern technology".* Retrieved 04/11/2025, from https://www.swissbanking.ch/en/media-politics/opinions/the-key-is-combining-trustworthiness-with-modern-technology

itopia. (2025). *IT Cost Survey for Swiss Banks 2025.* Retrieved 09/10/2025, from https://www.itopia.ch/media/it_cost_survey_2025_en.pdf

Jesis, M. (2024). *Integrating Security as Code: A Necessity for DevSecOps.* Retrieved 16/10/2025, from https://gitprotect.io/blog/integrating-security-as-code-a-necessity-for-devsecops/

Kaib, B. (2008). *Outsourcing in Banken.* Gabler Verlag.

KPMG. (2023). *Financial Services in a Connected Ecosystem: The Future of FinTech.* Retrieved 04/11/2025, from https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/future-of-fintech-web-copy.pdf

KPMG. (2025). *KPMG Global Tech Report: Financial Services Insights.* Retrieved 04/11/2025, from https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/kpmg-tech-survey-financial-services-insights.pdf

L'Hostis, A. (2025). *How Emerging Tech Will Transform Digital Banking Experiences Over The Next Decade.* Retrieved 26/09/2025, from https://www.forrester.com/blogs/how-emerging-tech-will-transform-digital-banking-experiences-over-the-next-decade/

Lindberg, M., & Tegnvallius Boklund, J. (online). *The EU Data Act: Portability Obligations for Cloud Providers.* Retrieved 16/10/2025, from https://www.lexology.com/library/detail.aspx?g=9b52d8d4-0e16-44df-9cc3-8b589802e229

Lodha, A. (2025). *Middleware Re-engineered: An Effective Approach to Decouple a Complex Monolith.* Retrieved 23/09/2025, from https://medium.com/next-at-chase/middleware-re-engineered-an-effective-approach-to-decouple-a-complex-monolith-bfdeb51e829b

Merlini, M., Küpper, L., Hagen, S., Römer, D., Deluchi, M., & Oltramare, X. (2023). *Neo-Core vs. Incumbent Core Banking Systems: A Comparison.* Working Paper, Boston Consulting Group (BCG) Platinion. Retrieved 06/11/2025, from https://media-publications.bcg.com/Neo-Core-vs-Incumbent-Core-Banking-Systems-June-2023.pdf

Morrison, A. (2025). *Top Cybersecurity Trends in Finance and Accounting for 2025.* Retrieved 14/10/2025, from https://www.invensis.net/blog/latest-cybersecurity-trends

Moustakis, I. (2025). *16 DevOps Metrics You Should Be Tracking [DORA & Other].* Retrieved 16/10/2025, from https://spacelift.io/blog/devops-metrics

Murphy, H. (2025). *Increasing reliance on complex technology leaves banks vulnerable.* Retrieved 04/11/2025, from https://www.ft.com/content/c148d46f-8c6f-487e-b8d7-8e7b9eddc324

National Cyber Security Centre Switzerland. (2025). *Technology Considerations: SCION*. Technology Brief, National Cyber Security Centre (NCSC), Switzerland. Retrieved 04/11/2025, from https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/dokumentation/technologiebetrachtungen/Technologiebetrachtung-SCION-EN.pdf.download.pdf/Technologiebetrachtung-SCION-EN.pdf

Olden, E. (2025). *Multi-Cloud Identity Management for Financial Services.* Retrieved 15/10/2025, from https://www.strata.io/blog/identity-access-management/multi-cloud-identity-management-finserv/

Pacheco, M. (2024). *Cloud-Agnostic Application Development: Key Elements & Benefits.* Retrieved 16/10/2025, from https://www.tierpoint.com/blog/cloud-agnostic/

Patel, U. (2024). *Data Privacy and Security in Financial Services. Journal of Artificial Intelligence & Cloud Computing*, *3*(5). Retrieved 06/11/2025, from https://onlinescientificresearch.com/articles/data-privacy-and-security-in-financial-services.pdf

Popp, C. (2023). *Development of Core Banking Systems in Switzerland – A Market Overview.* Retrieved 04/11/2025, from https://www.swisscom.ch/en/business/enterprise/themen/banking/aktualisierung-der-systeme.html

PreEmptive. (online). *DevOps in Financial Services: Unlocking Efficiency and Security.* Retrieved 16/10/2025, from https://www.preemptive.com/blog/devops-in-financial-services-unlocking-efficiency-and-security/

Red Hat. (2023). *What is DevSecOps?* Retrieved 04/11/2025, from https://www.redhat.com/en/topics/devops/what-is-devsecops

Rhyner, U. (2023a). *Quo vadis Bank-IT: Drei strategische Optionen.* Retrieved 21/10/2025, from https://www.inventx.ch/blog/quo-vadis-bank-it-drei-strategische-optionen/

Rhyner, U. (2023b). *Referenz-Blueprints für die IT von Banken & Krankenkassen.* Retrieved 10/10/2025, from https://www.inventx.ch/blog/referenz-blueprints-fuer-die-it-von-banken-krankenkassen/

Riese, C. (2006). *Industrialisierung von Banken: Grundlagen, Ausprägungen, Wirkungen*. Springer.

Sarkar, S. (online). *Data Lakehouse vs. Data Fabric vs. Data Mesh.* Retrieved 15/10/2025, from https://www.ibm.com/think/topics/data-lakehouse-vs-data-fabric-vs-data-mesh

Scherenberg, F., Hellmeier, M., & Otto, B. (2024). *Data Sovereignty in Information Systems. Electronic Markets*, *34*. Retrieved 04/11/2025, from https://doi.org/10.1007/s12525-024-00693-4

Schär, F. (2021). *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review*, *103*(2), 153–174. Retrieved 04/11/2025, from https://doi.org/10.20955/r.103.153-74

Shivakumar, S. K., & Sethii, S. (2019). *Building Digital Experience Platforms*. Springer.

Shumsky, P. (2023). *Banks & Fintechs: Embracing an API-First Strategy with a Middleware Technology.* Retrieved 23/09/2025, from https://www.digitaljournal.com/business/banks-fintechs-embracing-an-api-first-strategy-with-a-middleware-technology/article

Sivaganeshan, L. (2025). *Deconstructing Middleware in Modern Banking: A Deep Dive into API Architecture.* Medium — WSO2 Solution Architecture Team Blog. Retrieved 29/10/2025, from https://medium.com/sa-team-blog/deconstructing-middleware-in-modern-banking-a-deep-dive-into-api-architecture-d3ab9a33e648

SIX. (2024). *What Is bLink – The Swiss Open Banking Platform.* Retrieved 29/10/2025, from https://docs.blink.six-group.com/docs/whats-blink/

Susnjara, S., & Smalley, I. (online). *What Is Hybrid Cloud Architecture?* Retrieved 15/10/2025, from https://www.ibm.com/think/topics/hybrid-cloud-architecture

Swiss Bankers Association . (2025). *Cloud Guidelines (3rd Edition).* Swiss Bankers Association. Retrieved 06/11/2025, from https://www.swissbanking.ch/_Resources/Persistent/c/3/7/8/c378dbe9e1dafa45f4e4f8783cacddf7436cd1e6/Cloud%20Guidelines%20%282025%29.pdf

Swiss Confederation. (2025). *e-ID Law Approved at the Ballot Box.* Retrieved 20/10/2025, from https://www.eid.admin.ch/en/e-id-gesetz-an-der-urne-angenommen-e

Swiss Financial Innovation Desk. (2025). *Financial Innovation in Switzerland - An Overview.* Retrieved 04/11/2025, from https://find.swiss/find-library/articles/financial-innovation-in-switzerland

Swiss Fintech Innovations. (2018). *Discussion Paper: Future Finance – The Future of Financial Institutions (View 2030).* Retrieved 29/10/2025, from https://swissfintechinnovations.ch/wp-content/uploads/2018/08/SFTI-Discussion-Paper_Future-Finance.pdf

Swisscom. (2023). *Core Banking Radar – SaaScada.* Retrieved 20/10/2025, from https://www.swisscom.ch/en/business/enterprise/themen/banking/core-banking-radar-saascada.html

Talati, D. (2025). *Secure Financial Data Lake Architecture: Balancing Regulatory Compliance and Analytics Capabilities. Journal of Information Systems Engineering and Management (JISEM).* Retrieved 04/11/2025, from https://jisem-journal.com/index.php/journal/article/view/12728

Tata Consultancy Services. (2011). *PostFinance, Switzerland to Deploy Integrated TCS BaNCS Banking Suite.* Retrieved 29/10/2025, from https://www.tcs.com/who-we-are/newsroom/press-release/postfinance-switzerland-integrated-tcs-bancs-banking-suite

Thürig, J., Cruz, C., & Xiao, M. (2025). *Agentic AI ind BFSI: Turning Vision into Value.* Retrieved 04/11/2025, from https://www.tenity.com/agentic-ai-report

ti&m. (2023). *Vertical integration thanks to modular neo-core banking systems.* Retrieved 06/11/2025, from https://www.ti8m.com/en/blog/vertikale-integration-neo-kernbankensysteme

Tunçer, T., Popp, C., Eckert, C., & Zerndt, T. (2025). *Core Banking Radar 2025.* Retrieved 13/10/2025, from https://www.swisscom.ch/en/business/enterprise/themen/banking/core-banking-radar-2025.html

World Economic Forum. (2018). *The New Physics of Financial Services: How Artificial Intelligence Is Transforming the Financial Ecosystem.* Retrieved 04/11/2025, from https://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf

World Economic Forum. (2025a). *Artificial Intelligence in Financial Services.* Retrieved 04/11/2025, from https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf

World Economic Forum. (2025b). *The Future of Global Fintech: From Rapid Expansion to Sustainable Growth (Second Edition).* Retrieved 04/11/2025, from https://reports.weforum.org/docs/WEF_Future_of_Global_Fintech_Second_Edition_2025.pdf

Young, J. (2024). *The 2024 Complete Core Banking Checklist.* Retrieved 04/11/2025, from https://www.csiweb.com/what-to-know/content-hub/blog/the-complete-core-banking-checklist/

**Lucerne School of Business**
Institute of Financial Services Zug IFZ
Campus Zug-Rotkreuz
Suurstoffi 1
6343 Rotkreuz

T +41 41 757 67 67
ifz@hslu.ch
hslu.ch/ifz

**A study conducted by**

HSLU Lucerne University of Applied Sciences and Arts

AACSB ACCREDITED

ISBN-Number
978-3-907379-59-2