Accessing the Untapped Potential of Large Language Models in Banking: A Capability Readiness Framework

Philipp Winder[1,*]

[1] Institute of Behavioral Science & Technology, University of St.Gallen, St. Gallen, Switzerland

* Corresponding author (philipp.winder@unisg.ch)

Abstract

This paper presents a novel capability-based framework for assessing organizational readiness in deploying large language models (LLMs) in the banking sector. While LLMs offer significant potential across domains such as customer service, compliance, and risk assessment, banks face unique deployment challenges due to regulatory constraints, legacy systems, and data sensitivity. Building on the dynamic capability view and adapting maturity levels from the Capability Maturity Model Integration (CMMI), the framework identifies and structures the organizational, contextual, and technical capabilities necessary for effective LLM deployment. It introduces a maturity-scaled self-assessment tool that enables banks to evaluate their current LLM readiness, diagnose capability gaps, and guide strategic investment decisions. Although developed for banking, the framework offers conceptual relevance to other high-stakes, highly regulated sectors.

Keywords: LLM, banking, dynamic capability view, digital transformation, strategy

1. Introduction

The banking sector is undergoing a significant transformation driven by the rapid advancement of large language models (LLMs). Recent estimates suggest that LLMs could generate between $200 billion and $340 billion in annual value (equivalent to 9 to 15% of the industry's operating profits), primarily through gains in productivity (Kamalnath et al. 2023). In addition to productivity gains, LLMs offer substantial potential for generating new revenue streams through innovative products and services (Carpenter 2020, Birch and Rutter 2023, Fares et al. 2023, Zhu et al. 2024, Ho and Chow 2024). As customer expectations for consistent, convenient, and personalized experiences continue to rise, the ability to deliver tailored interactions becomes a key differentiator (Chung et al. 2020, Carpenter 2020). Customers who report the best experiences spend up to 140% more in general (Kriss 2014), and banks with the highest level of customer satisfaction have achieved deposit growth rates 84% faster than their peers (Chung et al. 2020). To capture this potential, banks must develop new value streams through intelligent, personalized offerings, innovative services, and streamlined omnichannel journeys (Thomas 2021). LLMs can serve as critical enablers of these capabilities (Demyttenaere et al. 2024, Ramamurthy et al. 2024, O'Brien and Downie 2024). This potential becomes even more vital in the competitive banking environment where roughly 58% of banks globally earn returns on equity that do not cover their cost of equity and where competitive threats from neobanks and nonbank challengers (e.g., big tech) continue to intensify (Bhattacharyya et al. 2023). In this context, the adoption of LLMs and the associated gains in productivity and innovative revenue streams offer a strategic opportunity to improve performance and stay ahead of the competition. Reflecting this, 86% of banks are either already in production or preparing to launch LLM-based use cases (Ramamurthy et al. 2024), and the banking industry was projected to be among the top two sectors in AI spending by the end of 2024 (Mettrick 2024). However, only 8% of banks are pursuing a systematic, enterprise-wide approach to LLM adoption, while the majority (72%) follow a tactical and fragmented approach (Ramamurthy et al. 2024). This fragmented approach poses a

challenge, as without strategic integration, LLM investments risk failing to deliver their full value. Effective deployment requires aligning LLM capabilities with core organizational processes and treating it as a core competence (Borges et al. 2021, Mikalef et al. 2023). Historically, incumbent banks have struggled to drive such strategic innovations, resulting in approximately 40% less productivity than digital-native neobanks (Babbar et al. 2023). These high failure rates stem from the sector's distinctive reliance on legacy systems, institutional risk aversion, silo-thinking, high regulatory requirements, and a limited ability to attract critical technological talent.

Thus, while LLMs offer significant upside potential for banks, both in terms of productivity gains and new revenue streams, the successful realization of this potential remains uncertain. Digital transformation efforts in banking have historically faced high failure rates or have been less effective than those of digital-native competitors (Babbar et al. 2023), and the deployment of LLMs is unlikely to be an exception. Although existing research has addressed specific challenges related to LLMs (e.g., privacy issues) or broader digital transformation (e.g., algorithm aversion) and has shown that technical resources need to be transformed to capabilities (Gupta et al. 2020, An et al. 2024), an integrated perspective on the capabilities required for successful LLM deployment in banking is lacking. A structured capability perspective specific to LLMs would enable banks to benchmark their current LLM readiness, guide the systematic development of critical capabilities, and ultimately reduce the risk of failure associated with digital transformation efforts in banking.

This paper addresses this gap by proposing a Banking LLM Capability Readiness Framework. Drawing on and synthesizing research streams from strategic management and information systems, the framework aims to provide a structured understanding of the organizational, contextual, and technical capabilities required to implement LLMs effectively in the banking sector. By combining the dynamic capability view (Teece et al. 1997, Eisenhardt and Martin 2000) with maturity levels adapted from the Capability Maturity Model Integration (CMMI) (CMMI Institute 2025), the framework not only identifies which capabilities are relevant

but also how they evolve (from fragmented experimentation to embedded, auditable, and continuously improving practices). Furthermore, the framework presents a set of questions for each capability, which are rated according to their maturity level, allowing banks to self-assess their LLM readiness. These questions serve as diagnostic and strategic orientation tool. In doing so, the framework provides a basis for theory-informed LLM capability building and offers a practical framework for evaluating, benchmarking, and prioritizing LLM deployment efforts across banks.

The remainder of the paper proceeds as follows. The next section presents the Banking LLM Capability Readiness Framework in detail. It introduces the capability categories, defines each capability, and outlines the associated assessment questions that operationalize the framework for practical use. The section also explains the underlying maturity levels for capability evaluation. The paper concludes with a discussion of the implications for research and practice, as well as suggestions for future work.

2. Banking LLM Capability Readiness Framework

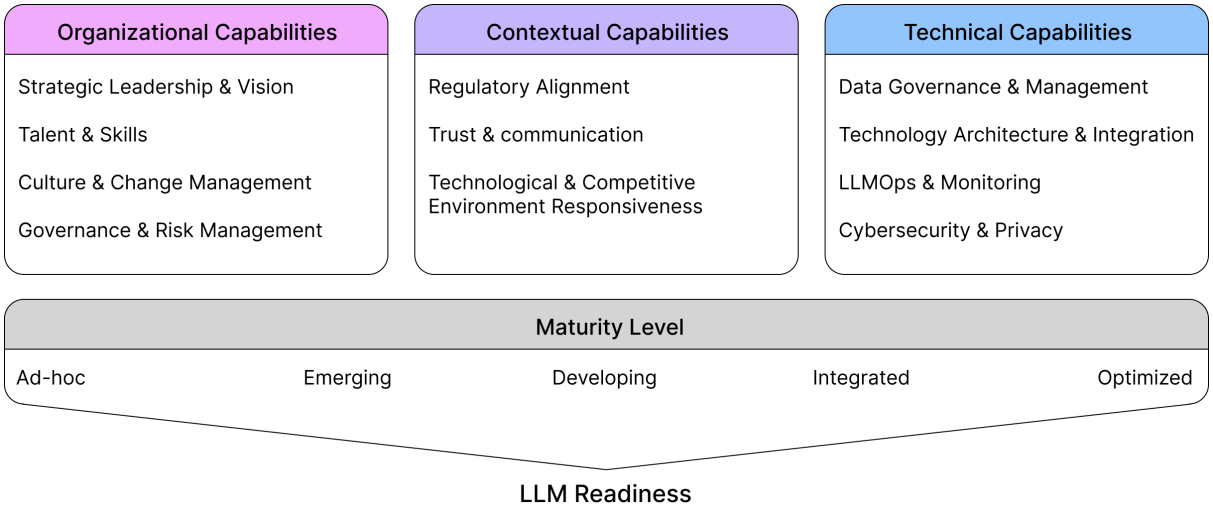
The Banking LLM Capability Readiness Framework builds on the dynamic capability view, which conceptualizes dynamic capabilities as the firm's capacity to "integrate, build, and reconfigure internal and external competencies to address rapidly changing environments" (Teece et al. 1997, p. 516). In line with this view, successful LLM deployment in banking requires more than access to technical resources. It depends on a bank's ability to develop dynamic capabilities across multiple domains, such as governance and leadership support. To capture this multi-dimensionality, the Banking LLM Capability Readiness Framework distinguishes between organizational, contextual, and technical capabilities. This subdivision reflects the underlying foundations of dynamic capabilities, which encompass not only technology-related competencies but also managerial processes, human capital, governance routines, and strategic alignment (Teece et al. 1997, Teece 2007, Gupta et al. 2020). Accordingly, (1) organizational capabilities in the framework relate to leadership, talent, change management, and governance, while (2) contextual capabilities reflect regulatory fit,

trust, and the competitive environment, and (3) technical capabilities include the data, architectures, and model operations enabling LLM use. These capabilities form the basis for long-term competitive advantage, particularly in fast-evolving, knowledge-intensive environments such as banking, by allowing banks to sense opportunities, seize them effectively, and continuously reconfigure their underlying resources in response to technology and competitive environment shifts (Teece et al. 1997, Eisenhardt and Martin 2000, Teece 2007, Schilke 2014). To account for variation in capability readiness, the framework also incorporates five maturity levels: Ad-hoc, emerging, developing, integrated, and optimized. These levels are adapted from the CMMI maturity model (CMMI Institute, 2025) and capture the evolutionary path from siloed experimentation (ad hoc capabilities) to fully institutionalized and auditable LLM usage (optimized capabilities). The framework thereby serves not only as an analytical tool for assessing a bank's current LLM readiness but also as a strategic orientation tool that supports the development of LLM capabilities over time.

To support the practical application, the framework includes a structural self-assessment tool comprising three diagnostic questions per capability (to ensure equal weighting of questions within a capability), each rated on the maturity levels. The tool enables banks' top management and digital transformation project leaders to efficiently evaluate their LLM readiness comparably, identify capability gaps, and prioritize investment areas. The tool is accessible at https://ibtphilipp.github.io/banking-llm-framework/. While the tool facilitates structured benchmarking and capability gap identification, it does not offer a prioritized implementation roadmap. It relies on self-reported assessments of broader, relevant capabilities, which may limit its ability to objectively evaluate a firm's actual LLM readiness.

Fig. 1 provides an overview of the Banking LLM Capability Readiness Framework. In the subsequent sections, all capabilities and maturity levels are introduced and explained in detail.

Fig 1. Overview of the Banking LLM Capability Readiness Framework.



2.1. Organizational Capabilities

Within the Banking LLM Capability Readiness Framework, organizational capabilities constitute a core element. While technical and contextual capabilities matter, the ability to successfully initiate, scale, and institutionalize LLM use depends primarily on how well an organization can lead, staff, initiate, and govern these efforts. This is reflected in the dynamic capability view, which emphasizes that competitive advantage in dynamic environments is not solely a consequence of resource ownership but stems from the ability to reconfigure and consciously align these resources (Teece et al. 1997, Eisenhardt and Martin 2000, Teece 2007).

First, *Strategic Leadership & Vision* are required to move beyond LLM experimentation. LLM initiatives need to be embedded in the business strategy. This includes a clear understanding of the expected returns (which have historically posed a particular problem for the banking sector; Babbar et al. 2023) and the capacity to allocate (financial and human) resources effectively. Second, *Talent & Skills* are essential for reducing organizational uncertainty around technology. Banks must ensure that key decision-makers and the affected workforce gain a thorough understanding of LLMs. This may involve building internal expertise through lighthouse projects, targeted upskilling, and selective hiring. As shown by prior research, the adoption of technology does not lead to performance improvements unless

supported by human capital and interpretative capacity (Hitt et al. 2001, Gupta et al. 2020). In the past, the banking sector struggled to attract relevant technological talent (Babbar et al. 2023). Third, *Culture & Change Management* further enables the adoption and institutionalization of LLMs. Executive-level support, cross-functional collaboration, and active employee engagement are necessary to move from isolated experimentation to sustained use. In the risk-averse banking context, this capability poses a significant hurdle. Finally, *Governance & Risk Management* ensures that the deployment of LLMs aligns with internal and external accountability requirements.

Taken together, these organizational capabilities determine whether LLM efforts remain isolated or evolve into scalable and reliable components of the bank's operating model. Their absence not only limits the effectiveness of technical investments but also increases the likelihood of LLM implementation failure, potentially resulting in a strategic disadvantage in an increasingly competitive banking environment (see Introduction).

2.1.1.Strategic Leadership & Vision

Strategic leadership and vision represent a foundational organizational capability for successful LLM deployment. Prior research on digital transformation and strategic alignment highlights that top-management involvement is critical to ensure that LLM investments are not only initiated but also embedded into a firm's strategy (Baker et al. 2011, Sabherwal et al. 2019, Tona et al. 2025). In banking, this includes defining the strategic role of LLMs, approving and sequencing projects, allocating resources, and ensuring coherence with corporate objectives across both retail and corporate business lines (Demyttenaere et al. 2024). Without a guiding vision and top-management support, LLM initiatives remain fragmented and fail to scale (Sabherwal et al. 2019).

Strategic alignment research further emphasizes that strategic alignment is not only the fit between strategy and technology but a dynamic capability that must be built, maintained, and adapted through executive leadership, shared planning processes, and iterative learning (Schwarz et al. 2010, Baker et al. 2011). Especially in a competitive environment characterized

by regulatory uncertainty and rapid technological change, sustained strategic alignment enables firms to adapt LLM investments in a structured and responsive manner (Sabherwal et al. 2019). This underscores the need for banks to move from isolated pilot LLM projects to strategy-driven LLM initiatives with tangible business value. Such a structured approach involves prioritizing LLM use cases based on value, effort, and risk and developing strategic roadmaps (Baecker et al. 2024, O'Brien and Downie 2024).

From a dynamic capability view, strategic leadership is also crucial to the orchestration of financial, human, and technological resources over time (Teece et al. 1997, Eisenhardt and Martin 2000, Teece 2007). In the context of LLMs, this includes identifying opportunities, directing investments, and transforming organizational routines to facilitate the use of LLMs. Thus, this orchestration requires continuous top-management engagement in capability building, learning, and cross-functional alignment (Barney 1991).

For practice, this implies that LLM readiness depends not only on whether banks have a vision but also on whether that vision is translated into a strategic LLM roadmap and respective resource allocations. Thereby, banks must avoid focusing exclusively on near-term automation benefits and instead define the role of LLMs in shaping products, services, and operating models (Nerijus et al. 2023). Strategic leadership and a vision provide the direction and coherence required to drive scalable, value-generating LLM use.

Table 1. Strategic Leadership & Vision Assessment Questions

Question
To what extent is LLM adoption guided by a clearly articulated strategic vision from senior leadership?
How consistently are LLM initiatives aligned with broader digital transformation objectives?
Is there an established process for sensing, evaluating, and responding to emerging LLM opportunities?

2.1.2. Talent & Skills

Developing relevant talent and skills is essential for transforming LLM deployment in banking from experimentation into a sustainable competitive advantage. Prior research highlights that banks must invest in workforce development to complement their technological investments (Chowdhury et al. 2024, Tona et al. 2025). Banks can only realize the potential of LLMs if they possess the ability to continuously build, adapt, and reconfigure human capital to meet the evolving technological demands (Barney 1991, Teece 2007). In the case of LLMs, this includes technical expertise, such as data engineering or prompt design, as well as managerial skills that enable employees to manage risk, interpret LLM outputs, and align implementation with the business strategy (An et al. 2024). The combination of technical and managerial LLM skills enables banks to move beyond experimentation and build scalable, strategy-aligned LLM applications. Literature on human-AI collaboration further highlights that these skills must be dynamic, as the continuous evolution of LLMs requires the continuous adaption of workforce skills (Chowdhury et al. 2024).

This dynamic nature requires banks to build talent and skills through two approaches. First, they need to invest in targeted upskilling initiatives for IT and business employees. Prior research shows that talent and skill development through continuous learning, peer training, and internal knowledge-sharing mechanisms (e.g., cross-functional learning communities) is more effective than relying solely on external hiring (Kane 2019, Neeley and Leonardi 2022, Braojos et al. 2024). Second, banks need to hire suitable talent and foster an environment in which LLM-related skills can be integrated into everyday decisions (e.g., enabling risk teams to evaluate LLM outputs). These approaches help build bank-specific human capital that is difficult to imitate and thus a strategically valuable organizational capability (Barney 1991, Pedraza-Rodríguez et al. 2023, An et al. 2024).

Therefore, talent and skills are not only a support function but a dynamic capability that allows banks to deploy LLMs in a context-sensitive and suitable manner.

Table 2. Talent & Skills Assessment Questions

Question
Does the bank have in-house expertise in LLM development, integration, and risk management?
Are training and reskilling programs in place to prepare staff for LLM-enabled workflows?
To what extent are cross functional teams empowered to innovate, validate, and scale LLM solutions?

2.1.3. Culture & Change Management

A growing research stream shows that digital transformation efforts often fail due to cultural inertia, which is particularly the case in incumbent organizations like banks, where legacy systems, risk aversion, and hierarchical structures dominate (Martínez-Caro et al. 2020, Grover et al. 2022, An et al. 2024, Braojos et al. 2024). An organizational culture that promotes openness, experimentation, and cross-functional collaboration is essential for successfully deploying technological innovations (Grover et al. 2022, An et al. 2024). Organizations with a strong continuous learning orientation and high digital adaptability are more likely to integrate LLMs into business operations and realize innovation advantages (Chowdhury et al. 2024). Without an organizational culture that promotes innovation, LLM initiatives remain disconnected from the organizational routines, which limits their effectiveness.

Successful change also depends on formal and informal processes that help employees understand, accept, and co-create the transformation (Robertson et al. 2025). Resistance to change in an organization can stem from uncertainty, anxiety, or a perceived loss of control (Tona et al. 2025, Robertson et al. 2025). Addressing these concerns requires more than training and visible leadership support (Kotter 1995). It involves creating a culture of psychological safety, inclusion, and shared purpose, where LLMs are understood as augmenting rather than replacing (Chowdhury et al. 2024, Sarala et al. 2025, Robertson et al. 2025).

Culture and change management define whether LLM deployment is treated as a narrow technical tool or as an opportunity to transform how the bank generates and captures value.

Table 3. Culture & Change Management Assessment Questions

Question
How receptive is the organizational culture to adopting LLM-based systems?
Are structured management processes in place to support LLM integration across business units?
To what extent are employees actively engaged in LLM-related initiatives and transformation?

2.1.4. Governance & Risk Management

Governance and risk management are a critical capability for responsible and sustainable LLM deployment in banking. LLMs introduce new risks, including discrimination (e.g., reinforcing social stereotypes), information hazards (e.g., private data leakage), misinformation harms (e.g., hallucinations), malicious use (e.g., new cybersecurity threats), human-computer interaction harms (e.g., amplified nudging in human-like conversations), and environmental and socioeconomic harms (e.g., environmental harms from operating LLMs), that cannot be managed through technical controls alone (Mittelstadt 2019, Weidinger et al. 2021, Mökander et al. 2024). In banking, where decisions are high-stakes, opaque, and highly regulated, these risks demand a structured and proactive governance approach.

Therefore, principles such as explainability, accountability, fairness, and transparency are insufficient if not operationalized through designated roles, documented processes, independent oversight, and clear documentation (Mitchell et al. 2019, Mittelstadt 2019, Weidinger et al. 2021, Mökander et al. 2024). Given their systemic importance and regulatory exposure, banks must adopt governance frameworks that extend beyond mere compliance and embed fiduciary responsibility and accountability (Cumming et al. 2021). The governance approach and auditing needs to span from pre-deployment testing to post-deployment monitoring on model, provider, and application levels (Mökander et al. 2024). Critically, the governance approach must be dynamic and capable of adapting to new risks that emerge from LLM technology innovations (Raji et al. 2020).

While internal governance provides the foundation, alignment with external regulatory requirements remains critical. Banks must ensure that their governance approaches are compatible with regulatory standards (see contextual capability *Regulatory Alignment*).

Ultimately, governance needs to be embedded within the core organizational processes rather than treated as a compliance afterthought. Effective governance enables banks to scale LLMs responsibly while protecting the bank, its customers, stakeholders, and the integrity of the financial system.

Table 4. Governance & Risk Management Assessment Questions

Question
Are there defined roles and responsibilities for governing LLM use within the bank?
To what extent are model risks (e.g., biases) systematically assessed and mitigated?
How comprehensively are LLM activities documented, audited, and aligned with risk policies?

2.2. Contextual Capabilities

Contextual capabilities describe a bank's ability to align LLM initiatives with external conditions and expectations. While organizational and technical capabilities constrain what a bank can build and operate internally, contextual capabilities shape whether these efforts are appropriate, timely, and strategically positioned within the banking environment. They determine the extent to which LLM use is aligned with regulatory requirements, trusted by internal and external stakeholders, and responsive to shifts in the technological and competitive landscape. Following the dynamic capability view, sustaining a competitive advantage in volatile environments requires not only internal resource orchestration but also continuous engagement and adaptation to external change (Teece et al. 1997).

Regulatory Alignment is an increasingly critical capability since the deployment of LLMs in banking is subject to evolving legal and compliance standards, including data protection laws, LLM-specific regulations (e.g., EU AI Act), and sector-specific regulations. Banks must, therefore, not only be aware of relevant regulatory developments but also possess the internal

capability to interpret, translate, and operationalize them in the context of LLM use. Failure to do so can lead to legal risk, reputational damage, or delays in LLM deployment. *Trust & Communication* shape whether stakeholders, ranging from employees to customers, accept and adopt LLMs. Prior research highlights that trust in LLMs is not inherent and needs to be actively cultivated (Dietvorst et al. 2015, Rai 2020). This includes both internal communication strategies to create transparency around the purpose and boundaries of LLMs, as well as external communication to ensure that customers and regulators remain confident in the bank's ability to use LLMs responsibly. Furthermore, *Responsiveness to Technological & Competitive Environments* is required to translate LLM technology innovations into a strategic advantage, leveraging higher productivity and new revenue streams (for details, see the Introduction). This encompasses the ability to sense relevant technological innovations, evaluate their strategic fit, and respond to shifts in customer expectations or competitor behavior. Such adaptive responsiveness characterizes dynamic capabilities (Teece et al. 1997) and distinguishes banks that adapt and thrive from those that remain path-dependent.

Contextual capabilities ensure that LLM adoption is not only feasible but also externally legitimate, strategically situated, and adaptive. Without them, even well-designed technical solutions risk misalignment with the law, a lack of stakeholder support, or irrelevance in a rapidly evolving competitive sector.

2.2.1. Regulatory Alignment

Since LLMs might be deployed in banking in sensitive domains such as credit scoring, fraud detection, and customer interaction, regulatory alignment becomes a critical contextual capability. Regulatory alignment addresses how banks interpret, operationalize, and adapt to external regulations governing LLM systems. Effective LLM adoption requires not only technical capabilities but also deep integration of evolving legal expectations into the governance approach (Cumming et al. 2021, Feretzakis et al. 2025). Banks must navigate a fragmented and multi-layered regulatory landscape, spanning general data protection (e.g.,

GDPR), financial regulation (e.g., MiFID, CFPB), and emerging AI-specific regulations (e.g., EU AI Act).

At the core of this capability is the establishment of ongoing legal oversight throughout the LLM lifecycle. Global banks must align with jurisdiction-specific regulations, including binding legislation in the EU (European Parliament 2024) and China (Cyberspace Administration of China et al. 2023), and more open (principle-based) approaches in the US (The White House 2025) and UK (Secretary of State for Science, Innovation and Technology 2023). While these vary in scope and legal force, they increasingly converge around risk-based and human-centric LLM principles. For example, the EU AI Act classifies multiple LLM applications in banking, including credit scoring, customer due diligence, and fraud detection, as “high-risk systems” (European Parliament 2024). This classification entails strict requirements regarding transparency, human oversight, risk management, and technical documentation.

Regulatory alignment complements the internal routines and protections included in the organizational capability of *Governance & Risk Management*. Without robust external regulatory alignment, even well-governed systems may fail to meet legal expectations, exposing banks to fines, operational restrictions, or loss of public trust.

Table 5. Regulatory Alignment Assessment Questions

Question
Is the bank systematically assessing LLM use cases against applicable regulatory requirements (e.g., GDPR)?
Are regulatory safeguards such as explainability and human oversight embedded in LLM systems?
How actively does the bank engage with regulators or industry bodies on LLM governance issues?

2.2.2. Trust & Communication

Trust and communication extend the organizational capability of *Culture & Change Management* by addressing how trust in LLMs is built and sustained internally among employees and externally among customers, regulators, other stakeholders, and the public.

Especially in banking, where decisions are high-stakes, perceptions of transparency, reliability, and control are critical for adoption and the protection of the bank's legitimacy.

Prior research shows that users often resist LLM-generated outputs, particularly in tasks involving affective trust (Hildebrand and Bergner 2021). However, this so-called algorithm aversion can be mitigated through careful system framing, visible human oversight, and decision-support positioning rather than full automation (Dietvorst et al. 2015, Zehnle et al. 2025). Trust increases when LLMs explain how inputs shape outputs (i.e., explainable AI and transparency), allow user interaction, and offer rationales in accessible language (Sakai and Nagai 2022, Bertrand et al. 2023, Zhu et al. 2024, Wang et al. 2024).

Trust in LLMs varies across user groups. Younger, digital-native users are generally more accepting of LLM-driven applications, whereas older or risk-averse users demand clearer safeguards and explanations (Lourenço et al. 2020, Figà-Talamanca et al. 2022, Zhu et al. 2024). Internal resistance is especially pronounced among senior staff in compliance or risk functions, who are more sensitive to model opacity and its implications for accountability (Wang et al. 2024).

Anthropomorphic design (i.e., human-like features, such as avatars) can support early adoption by increasing social presence but may reduce perceived credibility in complex tasks (Hildebrand and Bergner 2021, Zhu et al. 2024). Thus, banks should calibrate design choices to task complexity and user expectations, avoiding over-personification in sensitive contexts.

Ultimately, trust in LLMs is not solely driven by the accuracy of LLMs (Wang et al. 2024). It requires a combination of explainability, perceived control, and consistent communication. Internally, training and transparency about system limitations support user confidence and responsible use. Externally, clear messaging reinforces trust.

Table 6. Trust & Communication Assessment Questions

Question
How effectively does the bank communicate the purpose, limitations, and safeguards of LLM usage to internal and external stakeholders?
Are mechanisms such as explainability, transparency, and user control consistently implemented?
To what extent are trust-related concerns (e.g., algorithm aversion, perceived autonomy) actively managed?

2.2.3. Technological & Competitive Environment Responsiveness

Technological and competitive environment responsiveness is a contextual capability that enables banks to sense and adapt to shifts in LLM technology, customer expectations, and market dynamics. In an environment shaped by rapid LLM advances, rising customer expectations, and increasing competition from fintechs and big tech, banks must align LLM use with evolving business models and customer needs (Chung et al. 2020, Carpenter 2020, Birch and Rutter 2023, Grimwade 2023). This includes tailoring LLM applications to market segments (e.g., retail vs. corporate) and balancing short-term efficiency gains with long-term innovation, which is often deprioritized under competitive pressure (Cao et al. 2024).

Responsiveness to the technological and competitive environment shapes which opportunities are pursued and how LLM strategy remains relevant in a dynamic environment (Rai et al. 2019). Additionally, it informs and enables the organizational capability of *Strategic Leadership & Vision*.

Table 7. Technological & Competitive Environment Responsiveness Assessment Questions

Question
How rapidly can the bank scale or adapt LLM systems in response to competitive or technological shifts?
Are LLM investments and architectures aligned with evolving platform ecosystems and open banking trends?
To what extent are decisions about LLM exploration and exploitation guided by strategic foresight and market monitoring?

2.3. Technical Capabilities

Technical capabilities provide the operational foundations required to deploy and manage LLMs at scale. While organizational and contextual capabilities define the strategic, technology, and competitive fit, technical capabilities determine whether LLM initiatives can be implemented reliably and securely. In line with the dynamic capability view (Teece et al. 1997, Eisenhardt and Martin 2000, Teece 2007), these capabilities enable the reconfiguration of technological assets to support sustained innovation and operational resilience.

First, *Data Governance & Management* ensures that LLMs are trained and operated on accurate, compliant, and contextually appropriate data. Second, *Technology Architecture & Integration* capabilities allow banks to flexibly embed LLMs within their IT architecture, balancing build-versus-buy decisions and managing interoperability with legacy systems. Third, *LLMOps* (LLM Operations) *& Monitoring* are required to maintain LLM operability and performance over time through deployment pipelines and logging. Finally, *Cybersecurity & Privacy* capabilities are critical in banking, where LLMs introduce novel risks and must operate within strict regulatory boundaries.

Taken together, technical capabilities define the operational feasibility of LLM initiatives.

2.3.1. Data Governance & Management

Data governance and management is a technical capability that integrates strategic oversight (governance) with operational execution (management) to ensure that data used across the LLM lifecycle (training, fine-tuning, prompting, inference) is accurate, secure, and fits the purpose. This capability directly supports *Governance & Risk Management* by enabling traceability, audibility, and regulator alignment.

Classical data quality research emphasizes that data “fitness for use” depends not only on accuracy but also on relevance, completeness, timeliness, and interpretability (Wang and Strong 1996). In LLM contexts, this translates to ensuring that data inputs (e.g., customer records, transaction histories, or laws) are use-case-relevant, well-structured, and trustworthy.

Furthermore, in high-stakes banking contexts, ensuring data provenance, clear source attribution, and representational transparency are of particular importance.

Recent work highlights the need for robust data governance practices like deduplication, cleaning, bias mitigation, and privacy-preserving techniques such as anonymization and access control (Meade et al. 2022, Ilyas and Rekatsinas 2022, Abbas et al. 2023, Montagna et al. 2023, Miao et al. 2024). These are essential in the banking environment, which is subject to privacy protection regulations (e.g., GDPR) (Feretzakis et al. 2024). At the same time, scalable data management systems are required to support data ingestion, normalization, augmentation, and inference (Feng et al. 2021, Miao et al. 2024). Data lifecycle challenges such as data refreshing and deletion remain unresolved in LLMs, posing significant compliance and reputational risks for banks (Miao et al. 2024, Feretzakis et al. 2025).

Taken together, data governance defines the standards and safeguards, while data management ensures they are met across LLM systems.

Table 8. Data Governance & Management Assessment Questions

Question
How consistently are data quality, integrity, and provenance assured across LLM use?
Are there formal processes for data access, anonymization, and data governance for LLM-relevant datasets?
To what extent are unstructured data assets (e.g., documents, chat logs) effectively leveraged for LLM use?

2.3.2. Technology Architecture & Integration

This capability supports the organizational capability *Strategic Leadership & Vision* by defining the technical infrastructure and integration that determines the speed, flexibility, and sustainability of LLM adoption.

Modern software architectures favor modularity, microservices, and containerization, enabling isolated deployment of components such as prompt libraries, policy engines, and model hubs (Tiwana et al. 2010, Newman 2015, Abd-Elwahab et al. 2023, Langer 2025, Weber et al. 2025). This modularity also facilitates updates, supports risk containment, and

enables horizontal scaling. It also aligns with platform ecosystem principles, where composable services enhance agility and interoperability (Tiwana et al. 2010, Benlian et al. 2018).

Integration with legacy banking systems remains a key challenge. Banks are increasingly relying on loosely coupled APIs, middleware, and caching-based workflows to utilize LLMs without disrupting core banking platforms (Simran and Geetha 2024, Staegemann et al. 2025). Additionally, hybrid deployment models, which combine cloud-based LLMs with on-premise data processing, gain traction due to data sovereignty and latency considerations (Blumberg et al. 2021, O'Brien and Downie 2024).

Strategic decisions such as build vs. partner or open source (e.g., Llama) vs. proprietary (e.g., ChatGPT) platforms must be guided by a structured assessment of architectural compatibility, scalability, and governance requirements (Kamalnath et al. 2023, Mettrick 2024). When pursuing a build strategy, ensuring scalability and performance requires architectural provisions for batching, GPU acceleration, and model distillation (i.e., transferring knowledge from a larger to a smaller LLM) (Hsieh et al. 2023, Koilia and Kachris 2024). In this case, performance monitoring, load balancing, and fault tolerance mechanisms are key for ensuring enterprise-grade resilience.

Given the sensitive nature of financial data, LLM architecture must embed security and privacy (see also *Cybersecurity & Privacy*).

Ultimately, this capability determines whether banks can evolve their IT ecosystem from static infrastructures into adaptive, LLM-ready platforms.

Table 9. Technology Architecture & Integration Assessment Questions

Question
Is the existing LLM architecture modular, scalable, and compatible with secure LLM integration?
To what extent are LLMs integrated with core systems via standardized APIs and middleware?
Are architectural decisions guided by governance, performance, explainability, and resilience requirements?

2.3.3. LLMOps & Monitoring

LLMOps and monitoring is a critical technical capability that enables banks to manage the full lifecycle of LLMs with the reliability, audibility, and compliance required in the banking context. It extends traditional MLOps (Machine Learning Operations) by addressing the scale, prompt sensitivity, and behavior of LLMs (Spirin and Balint 2023, Pahune and Akhtar 2025, Zarour et al. 2025).

LLMOps and monitoring encompass automated deployment pipelines, prompt and context versioning, and real-time monitoring of output quality, safety, and performance (Testi et al. 2022, Huang et al. 2024, Pahune and Akhtar 2025, Zarour et al. 2025). Unlike conventional ML systems, LLMs require tracking prompt changes and contexts as core elements of LLMOps.

In banking, LLMOps supports *Regulatory Alignment* by enabling reproducibility, version control, and rollback mechanisms (Barman et al. 2024, Zarour et al. 2025). It must also enable the detection of anomalies (e.g., hallucinations), which should trigger human-in-the-loop reviews. By embedding risk controls into continuous delivery pipelines, LLMOps ensure that model updates are bias-mitigated, interpretable, and legally compliant before deployment to production (Pahune and Akhtar 2025). Integrated with governance structures, LLMOps operationalizes oversight and directly support the organizational capability *Governance & Risk Management.*

Table 10. LLMOps & Monitoring Assessment Questions

Question
Are there established continuous integration/continuous deployment pipelines and monitoring systems tailored for LLM deployment and updates?
How effectively are performance, safety, and compliance issues detected and addressed post-deployment?
Are prompts, data sources, and LLM behaviors versioned, audited, and continuously evaluated?

2.3.4. Cybersecurity & Privacy

Deploying LLMs in banking requires the technical capability to protect data confidentiality, integrity, and compliance. This is particularly relevant for banking contexts, which are subject to pronounced regulatory constraints and cybersecurity threats. Therefore, banks need to establish robust cybersecurity and privacy-preserving data practices tailored to the unique risks of LLMs (Das et al. 2024, Raza et al. 2025).

From a cybersecurity perspective, LLMs introduce novel threats such as adversarial inputs (malicious prompts designed to bypass LLM security measures), model inversion (reconstruction of training data from model outputs), and prompt injection (inserting hidden prompt instructions to hijack LLM behavior) (Koball et al. 2024, Das et al. 2024, Kovacevic et al. 2024). These attacks can lead to manipulated outputs or the extraction of sensitive data. Banks must implement layered defenses to reduce LLM exposure and misbehavior. Such defenses include adversarial training (training LLMs on malicious inputs), input validation, as well as anomaly detection and red-teaming (simulating attacks to improve model security)(Ganguli et al. 2022, Perez et al. 2022, Das et al. 2024, Kovacevic et al. 2024). Secure storage, access control, and encrypted pipelines also mitigate internal misuse and external exploitation (Feretzakis et al. 2024, Das et al. 2024).

Privacy protection mechanisms are critical since LLMs are vulnerable to memorizing personally identifiable information, which makes differential privacy (protecting sensitive data by adding statistical noise), selective forgetting (removing specific data from a model's knowledge), and synthetic data generation (protecting sensitive information by creating artificial data that mimics real data) in the training necessary (Shokri et al. 2017, Weitzenboeck et al. 2022, Feretzakis et al. 2024). In high-stakes banking applications, compliance with privacy protection laws (e.g., GDPR, CCPA) demands pseudonymization (replacing personal identifiers with fictitious placeholders), data minimization, and privacy assessments (Lagioia and Sartor 2020, Das et al. 2024). However, fully anonymizing unstructured banking data remains operationally infeasible in many cases, making risk-based pseudonymization and

contextual access controls more practical (Lagioia and Sartor 2020, Weitzenboeck et al. 2022).

This capability directly reinforces the organizational capability *Governance & Risk Management* by operationalizing security-by-design and privacy-by-default principles. It requires close coordination with LLMOps, model governance, and compliance teams to ensure that technical safeguards align with regulations and internal controls. Further, it has direct implications for internal and external trust in LLM-based systems.

Table 11. Cybersecurity & Privacy Assessment Questions

Question
Are LLM systems protected against data leakage, adversarial attacks, and misuse across the lifecycle?
To what extent are privacy-preserving techniques (e.g., pseudonymization) adopted?
Is there a comprehensive security governance model covering LLM access, audit, and incident response?

2.4. Maturity Levels

To capture the heterogeneous state of LLM capabilities readiness across a bank, the framework incorporates five maturity levels: Ad-hoc, Emerging, Developing, Integrated, and Optimized. The maturity levels are inspired by the CMMI (CMMI Institute 2025), a widely used maturity model for IT management in the broader sense (Becker et al. 2009), the maturity levels have been slightly adapted to better reflect increasing degrees of formalization, institutional support, and strategic alignment and transformed from a six-level to five-level scale. The maturity levels are designed to be capability-agnostic. Each capability, whether organizational, contextual, or technical, can be assessed independently along the same five-level scale. This allows for granular diagnosis and benchmarking. A bank may, for example, exhibit integrated maturity in *Data Governance & Management* while remaining in an emerging state in *Culture & Change Management*. The maturity levels enable a systematic assessment

across capabilities, supporting targeted capability building. By identifying maturity gaps, banks can prioritize LLM development efforts.

Table 12. Maturity Levels.

Maturity Level	Capability-Agnostic Definition
Ad-hoc	**No formal processes, highly reactive.** Activities are informal, inconsistent, and typically limited to individual, isolated efforts or teams. No shared frameworks or repeatable processes are in place.
Emerging	**Initial efforts, informal practices.** Isolated initiatives have started. Basic tools, roles, or processes are introduced. Implementation remains fragmented.
Developing	**Defined processes, inconsistent execution.** Practices are coordinated and repeatable. Clear responsibilities exist, and structures or processes support business strategy. Performance is tracked to some extent.
Integrated	**Capabilities are coordinated and embedded.** Capability is embedded at the organizational level. Processes are standardized, outcomes are measured, and cross-functional collaboration is institutionalized. Risk controls and quality mechanisms are applied.
Optimized	**Continuous improvement and best practices.** Capability is continuously refined through feedback, monitoring, and innovation. Capability performance is proactively managed, and the bank can flexibly respond to regulatory, technological, or competitive shifts.

3. Conclusion

This practice-oriented paper provides a capability-based framework and assessment tool for evaluating the readiness of banks to deploy LLMs in a strategic, compliant, and scalable manner. Grounded in the dynamic capability view and extended through maturity levels adapted from the CMMI, the framework structures the complex requirements of LLM deployment into organizational, contextual, and technical capabilities. It further operationalizes these capabilities through maturity-scaled assessment questions that enable both diagnostic insight and strategic planning.

The framework supports banks in identifying organizational blind spots, aligning governance and risk structures with evolving LLM operations, and anticipating integration challenges linked to legacy systems, regulatory constraints, and data sensitivity. The maturity

levels add a dynamic, longitudinal lens that supports banks in assessing their LLM readiness and developing an LLM roadmap. The assessment tool offers a structural approach for prioritizing investments, sequencing capability development, and benchmarking progress over time.

The framework extends research on dynamic capabilities and technology adoption by integrating the dynamic capability view with evolutionary maturity levels, thereby offering a scalable model that can guide LLM capability development beyond the banking sector. While developed for banking, the framework may be adapted to other sectors that face similar constraints in terms of legacy systems, regulatory oversight, data sensitivity, and explainability, such as insurance or legal services. In other sectors, domain-specific extensions may be required, such as those for cyber-physical system integration in manufacturing.

Future work may further validate and refine the framework through empirical assessments, extend its applicability, or integrate it with financial performance indicators to evaluate the impact of LLM capability development. As LLMs continue to transform the banking sector, this framework provides a theoretical perspective and a practical tool for navigating the organizational complexity and strategic uncertainty associated with LLM adoption.

4. References

Abbas A, Tirumala K, Simig D, Ganguli S, Morcos AS (2023) SemDeDup: Data-efficient learning at web-scale through semantic deduplication. (March 22) http://arxiv.org/abs/2303.09540.

Abd-Elwahab AM, Mohamed AG, Shaaban EM (2023) MicroServices-driven enterprise architecture model for infrastructure optimization. Future Bus. J. 9(1):1–15.

An M, Lin J, Luo X (Robert) (2024) The impact of human AI skills on organizational innovation: The moderating role of digital organizational culture. J. Bus. Res. 182:114786.

Babbar A, Janardhanan R, Paternoster R, Soller H (2023) Why most digital banking transformations fail—and how to flip the odds (McKinsey & Company).

Baecker P, Helbig C, Shah R, Descamps G, Mehta B (2024) How Bank CIOs Can Build a Solid Foundation for Generative AI. Bain. Retrieved (September 17, 2024), https://www.bain.com/insights/how-bank-cios-can-build-a-solid-foundation-for-generative-ai/.

Baker J, Jones DR, Cao Q, Song J (2011) Conceptualizing the Dynamic Strategic Alignment Competency. J. Assoc. Inf. Syst. 12(4):299–322.

Barman KG, Wood N, Pawlowski P (2024) Beyond transparency and explainability: on the need for adequate and contextualized user guidelines for LLM use. Ethics Inf. Technol. 26(3):47.

Barney J (1991) Firm Resources and Sustained Competitive Advantage. J. Manag. 17(1):99–120.

Becker J, Knackstedt R, Pöppelbuß J (2009) Developing Maturity Models for IT Management. Bus. Inf. Syst. Eng. 1(3):213–222.

Benlian A, Kettinger WJ, Sunyaev A, Winkler TJ (2018) The Transformative Value of Cloud Computing: A Decoupling, Platformization, and Recombination Theoretical Framework. J. Manag. Inf. Syst. 35(3):719–739.

Bertrand A, Eagan JR, Maxwell W (2023) Questioning the ability of feature-based explanations to empower non-experts in robo-advised financial decision-making. Proc. 2023 ACM Conf. Fairness Account. Transpar. FAccT '23. (Association for Computing Machinery, New York, NY, USA), 943–958.

Bhattacharyya D, Dietz M, Edlich A, Höll R, Mehta A, Weintraub B, Windhagen E (2023) Global Banking Annual Review 2023: The Great Banking Transition (McKinsey & Company).

Birch DGW, Rutter K (2023) Where are the customers' bots? The AI paradigm shift in retail banking. J. Digit. Bank. 8(2):132–140.

Blumberg S, Isenberg R, Kerr D, Mitra M, Thomas R (2021) Beyond digital transformations: Modernizing core technology for the AI bank of the future (McKinsey & Company).

Borges AFS, Laurindo FJB, Spínola MM, Gonçalves RF, Mattos CA (2021) The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions. Int. J. Inf. Manag. 57:102225.

Braojos J, Weritz P, Matute J (2024) Empowering organisational commitment through digital transformation capabilities: The role of digital leadership and a continuous learning environment. Inf. Syst. J. 34(5):1466–1492.

Cao HH, Ma L, Ning ZE, Sun B (2024) How Does Competition Affect Exploration vs. Exploitation? A Tale of Two Recommendation Algorithms. Manag. Sci. 70(2):1029–1051.

Carpenter UT (2020) Revolutionising the consumer banking experience with artificial intelligence. J. Digit. Bank. 4(4):291–300.

Chowdhury S, Budhwar P, Wood G (2024) Generative Artificial Intelligence in Business: Towards a Strategic Human Resource Management Framework. Br. J. Manag. 35(4):1680–1691.

Chung V, Gomes M, Rane S, Singh S, Thomas R (2020) Reimagining customer engagement for the AI bank of the future (McKinsey & Company).

CMMI Institute (2025) CMMI Institute - CMMI Levels of Capability and Performance. Retrieved (May 13, 2025), https://cmmiinstitute.com/learning/appraisals/levels.

Cumming D, Girardone C, Śliwa M (2021) Corporate governance in extreme institutional environments. Br. J. Manag. 32(4):919–946.

Cyberspace Administration of China, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Public Security, National Radio and Television Administration (2023) Interim Measures for the Management of Generative Artificial Intelligence Service

Das BC, Amini MH, Wu Y (2024) Security and Privacy Challenges of Large Language Models: A Survey. (November 14) http://arxiv.org/abs/2402.00888.

Demyttenaere M, Roos A, Sheth H, Rodt M, Harris M, Fehling R, Martines D, Grabowski J (2024) Generative AI in the Finance Function of the Future (Boston Consulting Group).

Dietvorst BJ, Simmons JP, Massey C (2015) Algorithm aversion: People erroneously avoid algorithms after seeing them err. J. Exp. Psychol. Gen. 144(1):114–126.

Eisenhardt KM, Martin JA (2000) Dynamic Capabilities: What Are They? Strateg. Manag. J. 21(10/11):1105–1121.

European Parliament (2024) EU AI Act

Fares OH, Butt I, Lee SHM (2023) Utilization of artificial intelligence in the banking sector: a systematic literature review. J. Financ. Serv. Mark. 28(4):835–852.

Feng SY, Gangal V, Wei J, Chandar S, Vosoughi S, Mitamura T, Hovy E (2021) A Survey of Data Augmentation Approaches for NLP. Zong C, Xia F, Li W, Navigli R, eds. Find.

Assoc. Comput. Linguist. ACL-IJCNLP 2021 (Association for Computational Linguistics, Online), 968–988.

Feretzakis G, Papaspyridis K, Gkoulalas-Divanis A, Verykios VS (2024) Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review. Information 15(11):697.

Feretzakis G, Vagena E, Kalodanis K, Peristera P, Kalles D, Anastasiou A (2025) GDPR and Large Language Models: Technical and Legal Obstacles. Future Internet 17(4):151.

Figà-Talamanca G, Tanzi PM, D'Urzo E (2022) Robo-advisor acceptance: Do gender and generation matter? PLOS ONE 17(6):e0269454.

Ganguli D, Lovitt L, Kernion J, Askell A, Bai Y, Kadavath S, Mann B, et al. (2022) Red Teaming Language Models to Reduce Harms: Methods, Scaling Behaviors, and Lessons Learned. (November 22) http://arxiv.org/abs/2209.07858.

Grimwade M (2023) The potential impacts of the digital revolution on the operational risk profiles of banks. J. Risk Manag. Financ. Inst. 17(1):71–88.

Grover V, Tseng SL, Pu W (2022) A theoretical perspective on organizational culture and digitalization. Inf. Manage. 59(4):103639.

Gupta S, Drave VA, Dwivedi YK, Baabdullah AM, Ismagilova E (2020) Achieving superior organizational performance via big data predictive analytics: A dynamic capability view. Ind. Mark. Manag. 90:581–592.

Hildebrand C, Bergner A (2021) Conversational robo advisors as surrogates of trust: onboarding experience, firm perception, and consumer financial decision making. J. Acad. Mark. Sci. 49(4):659–676.

Hitt MA, Bierman L, Shimizu K, Kochhar R (2001) Direct and Moderating Effects of Human Capital on Strategy and Performance in Professional Service Firms: A Resource-Based Perspective. Acad. Manage. J. 44(1):13–28.

Ho SPS, Chow MYC (2024) The role of artificial intelligence in consumers' brand preference for retail banks in Hong Kong. J. Financ. Serv. Mark. 29(2):292–305.

Hsieh CY, Li CL, Yeh CK, Nakhost H, Fujii Y, Ratner A, Krishna R, Lee CY, Pfister T (2023) Distilling Step-by-Step! Outperforming Larger Language Models with Less Training Data and Smaller Model Sizes. (July 5) http://arxiv.org/abs/2305.02301.

Huang K, Manral V, Wang W (2024) From LLMOps to DevSecOps for GenAI. Huang K, Wang Y, Goertzel B, Li Y, Wright S, Ponnapalli J, eds. Gener. AI Secur. Theor. Pract. (Springer Nature Switzerland, Cham), 241–269.

Ilyas IF, Rekatsinas T (2022) Machine Learning and Data Cleaning: Which Serves the Other? J Data Inf. Qual. 14(3):13:1-13:11.

Kamalnath V, Lerner L, Moon J, Sari G, Sohoni V, Zhang S (2023) Capturing the full value of generative AI in banking (McKinsey & Company).

Kane G (2019) The Technology Fallacy. Res.-Technol. Manag. 62(6):44–49.

Koball C, Wang Y, Rimal BP, Vaidyan V (2024) Machine Learning Security: Threat Model, Attacks, and Challenges. Computer 57(10):26–35.

Koilia N, Kachris C (2024) Hardware Acceleration of LLMs: A comprehensive survey and comparison. (September 5) http://arxiv.org/abs/2409.03384.

Kotter JP (1995) Leading Change: Why Transformation Efforts Fail. Harvard Business Review https://hbr.org/1995/05/leading-change-why-transformation-efforts-fail-2.

Kovacevic A, Radenkovic SD, Nikolic D (2024) Artificial intelligence and cybersecurity in banking sector: opportunities and risks. (November 28) http://arxiv.org/abs/2412.04495.

Kriss P (2014) The Value of Customer Experience, Quantified. Harvard Business Review (August 1) https://hbr.org/2014/08/the-value-of-customer-experience-quantified.

Lagioia F, Sartor G (2020) The impact of the general data protection regulation on artificial intelligence (Publications Office of the European Union).

Langer AM (2025) Transforming Legacy Systems. Langer AM, ed. Anal. Des. -Gener. Softw. Archit. Gener. AI Cybersecurity Cloud Comput. (Springer Nature Switzerland, Cham), 221–258.

Lourenço CJS, Dellaert BGC, Donkers B (2020) Whose algorithm says so: The relationships between type of firm, perceptions of trust and expertise, and the acceptance of financial robo-advice. J. Interact. Mark. 49:107–124.

Martínez-Caro E, Cegarra-Navarro JG, Alfonso-Ruiz FJ (2020) Digital technologies and firm performance: The role of digital organisational culture. Technol. Forecast. Soc. Change 154:119962.

Meade N, Poole-Dayan E, Reddy S (2022) An Empirical Survey of the Effectiveness of Debiasing Techniques for Pre-trained Language Models. Muresan S, Nakov P,

Villavicencio A, eds. Proc. 60th Annu. Meet. Assoc. Comput. Linguist. Vol. 1 Long Pap. (Association for Computational Linguistics, Dublin, Ireland), 1878–1898.

Mettrick G (2024) The AI handbook for financial services leaders : Tips and tactics for mastering AI in banking and finance. J. Secur. Oper. Custody 16(3):286–296.

Miao X, Jia Z, Cui B (2024) Demystifying Data Management for Large Language Models. Companion 2024 Int. Conf. Manag. Data SIGMOD '24. (Association for Computing Machinery, New York, NY, USA), 547–555.

Mikalef P, Islam N, Parida V, Singh H, Altwaijry N (2023) Artificial intelligence (AI) competencies for organizational performance: A B2B marketing capabilities perspective. J. Bus. Res. 164:113998.

Mitchell M, Wu S, Zaldivar A, Barnes P, Vasserman L, Hutchinson B, Spitzer E, Raji ID, Gebru T (2019) Model Cards for Model Reporting. Proc. Conf. Fairness Account. Transpar. FAT* '19. (Association for Computing Machinery, New York, NY, USA), 220–229.

Mittelstadt B (2019) Principles alone cannot guarantee ethical AI. Nat. Mach. Intell. 1(11):501–507.

Mökander J, Schuett J, Kirk HR, Floridi L (2024) Auditing large language models: a three-layered approach. AI Ethics 4(4):1085–1115.

Montagna S, Ferretti S, Klopfenstein LC, Florio A, Pengo MF (2023) Data Decentralisation of LLM-Based Chatbot Systems in Chronic Disease Self-Management. Proc. 2023 ACM Conf. Inf. Technol. Soc. Good GoodIT '23. (Association for Computing Machinery, New York, NY, USA), 205–212.

Neeley T, Leonardi P (2022) Developing a Digital Mindset. Harvard Business Review https://hbr.org/2022/05/developing-a-digital-mindset.

Nerijus Z, Kirsten R, Alyssa L, Kapadia R (2023) AI in Financial Services: Making it happen at scale (BCG).

Newman S (2015) Building Microservices 1st ed. (O'Reilly Media, Inc.).

O'Brien K, Downie A (2024) What Is AI In Banking? | IBM. Retrieved (September 17, 2024), https://www.ibm.com/topics/ai-in-banking.

Pahune S, Akhtar Z (2025) Transitioning from MLOps to LLMOps: Navigating the Unique Challenges of Large Language Models. Information 16(2):87.

Pedraza-Rodríguez JA, Ruiz-Vélez A, Sánchez-Rodríguez MI, Fernández-Esquinas M (2023) Management skills and organizational culture as sources of innovation for firms in peripheral regions. Technol. Forecast. Soc. Change 191:122518.

Perez E, Huang S, Song F, Cai T, Ring R, Aslanides J, Glaese A, McAleese N, Irving G (2022) Red Teaming Language Models with Language Models. Proc. 2022 Conf. Empir. Methods Nat. Lang. Process. (Association for Computational Linguistics, Abu Dhabi, United Arab Emirates), 3419–3448.

Rai A (2020) Explainable AI: from black box to glass box. J. Acad. Mark. Sci. 48(1):137–141.

Rai A, Constantinides P, Sarker S (2019) Next generation digital platforms: toward human-AI hybrids. Manag. Inf. Syst. Q. 43(1):iii–ix.

Raji ID, Smart A, White RN, Mitchell M, Gebru T, Hutchinson B, Smith-Loud J, Theron D, Barnes P (2020) Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. Proc. 2020 Conf. Fairness Account. Transpar. FAT* '20. (Association for Computing Machinery, New York, NY, USA), 33–44.

Ramamurthy S, Duigenan JJ, Sironi P (2024) 2024 Global Outlook for Banking and Financial Markets - Regenerate banking with AI

Raza M, Jahangir Z, Riaz MB, Saeed MJ, Sattar MA (2025) Industrial applications of large language models. Sci. Rep. 15(1):13755.

Robertson J, Botha E, Oosthuizen K, Montecchi M (2025) Managing change when integrating artificial intelligence (AI) into the retail value chain: The AI implementation compass. J. Bus. Res. 189:115198.

Sabherwal R, Sabherwal S, Havakhor T, Steelman Z (2019) HOW DOES STRATEGIC ALIGNMENT AFFECT FIRM PERFORMANCE? THE ROLES OF INFORMATION TECHNOLOGY INVESTMENT AND ENVIRONMENTAL UNCERTAINTY. MIS Q. 43(2):453–474.

Sakai T, Nagai T (2022) Explainable autonomous robots: a survey and perspective. Adv. Robot. 36(5–6):219–238.

Sarala RM, Post C, Doh J, Muzio D (2025) Advancing Research on the Future of Work in the Age of Artificial Intelligence (AI). J. Manag. Stud. n/a(n/a).

Schilke O (2014) On the contingent value of dynamic capabilities for competitive advantage: The nonlinear moderating effect of environmental dynamism. Strateg. Manag. J. 35(2):179–203.

Schwarz A, Kalika M, Kefi H, Schwarz C (2010) A Dynamic Capabilities Approach to Understanding the Impact of IT-Enabled Businesses Processes and IT-Business Alignment on the Strategic and Operational Performance of the Firm. Commun. Assoc. Inf. Syst. 26:57–84.

Secretary of State for Science, Innovation and Technology (2023) A pro-innovation approach to AI regulation

Shokri R, Stronati M, Song C, Shmatikov V (2017) Membership Inference Attacks against Machine Learning Models. (March 31) http://arxiv.org/abs/1610.05820.

Simran T, Geetha J (2024) Enhancing Graph Database Interaction through Generative AI-Driven Natural Language Interface for Financial Fraud Detection. 2024 15th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 1–8.

Spirin N, Balint M (2023) Mastering LLM Techniques: LLMOps. NVIDIA Tech. Blog. Retrieved (May 24, 2025), https://developer.nvidia.com/blog/mastering-llm-techniques-llmops/.

Staegemann D, Haertel C, Daase C, Pohl M, Abdallah M, Turowski K (2025) A Review on Large Language Models and Generative AI in Banking. 267–278.

Teece DJ (2007) Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. Strateg. Manag. J. 28(13):1319–1350.

Teece DJ, Pisano G, Shuen A (1997) Dynamic capabilities and strategic management. Strateg. Manag. J. 18(7):509–533.

Testi M, Ballabio M, Frontoni E, Iannello G, Moccia S, Soda P, Vessio G (2022) MLOps: A Taxonomy and a Methodology. IEEE Access 10:63606–63618.

The White House (2025) Removing Barriers to American Leadership in Artificial Intelligence

Thomas R (2021) Introduction: Building the AI bank of the future | McKinsey. Retrieved (September 17, 2024), https://www.mckinsey.com/industries/financial-services/our-insights/introduction-building-the-ai-bank-of-the-future.

Tiwana A, Konsynski B, Bush AA (2010) Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. Inf. Syst. Res. 21(4):675–687.

Tona O, Leidner DE, van der Meulen N, Wixom B, Nunes J, Shagam D (2025) The Deployment of AI to Infer Employee Skills: Insights From Johnson & Johnson's Digital-First Workforce Initiative. Inf. Syst. J. n/a(n/a).

Wang RY, Strong DM (1996) Beyond Accuracy: What Data Quality Means to Data Consumers. J. Manag. Inf. Syst. 12(4):5–33.

Wang W, Gao G, Agarwal R (2024) Friend or Foe? Teaming Between Artificial Intelligence and Workers with Variation in Experience. Manag. Sci. 70(9):5753–5775.

Weber M, Hein A, Weking J, Krcmar H (2025) Orchestration logics for artificial intelligence platforms: From raw data to industry-specific applications. Inf. Syst. J. 35(3):1015–1043.

Weidinger L, Mellor J, Rauh M, Griffin C, Uesato J, Huang PS, Cheng M, et al. (2021) Ethical and social risks of harm from Language Models. (December 8) http://arxiv.org/abs/2112.04359.

Weitzenboeck EM, Lison P, Cyndecka M, Langford M (2022) The GDPR and unstructured data: is anonymization possible? Int. Data Priv. Law 12(3):184–206.

Zarour M, Alzabut H, Al-Sarayreh KT (2025) MLOps best practices, challenges and maturity models: A systematic literature review. Inf. Softw. Technol. 183:107733.

Zehnle M, Hildebrand C, Valenzuela A (2025) Not all AI is created equal: A meta-analysis revealing drivers of AI resistance across markets, methods, and time. Int. J. Res. Mark.

Zhu H, Vigren O, Söderberg IL (2024) Implementing artificial intelligence empowered financial advisory services: A literature review and critical research agenda. J. Bus. Res. 174:114494.