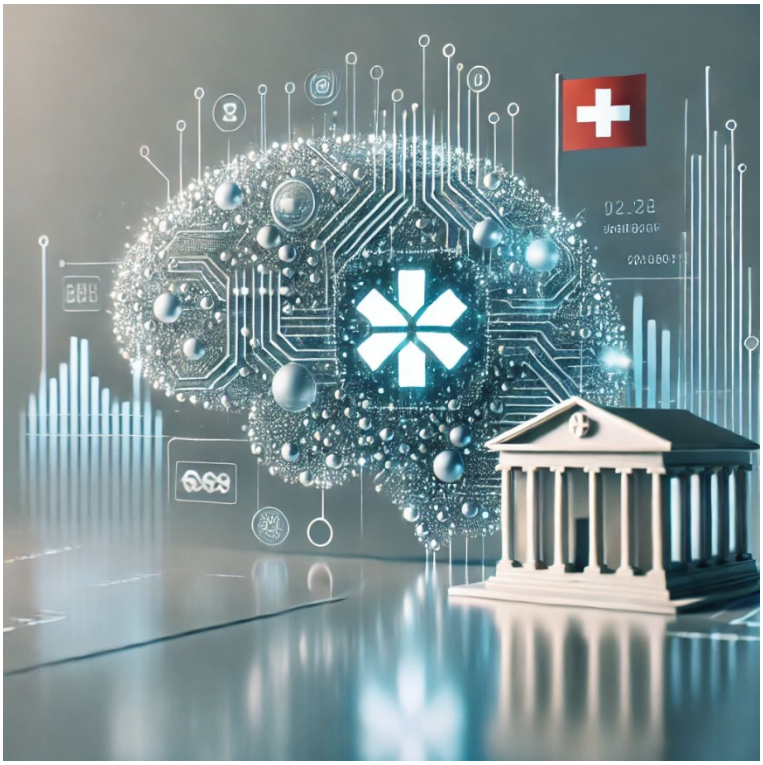
SFTI – working group 'Implementing AI'

'A Scalable Framework for Implementing Artificial Intelligence in Swiss Financial Institutions'

White Paper



Authorship: Swiss FinTech Innovations and Eastern Switzerland University of Applied Sciences
Release: Version 1.0
Date: 30.01.2025

Authors

OST Eastern Switzerland University of Applied Sciences, Institute for Finance & Law

Stefan Neumann

SFTI (Swiss Fintech Innovations)

Stephanie Wickihalder

About OST

Eastern Switzerland University of Applied Sciences (OST) is a dynamic, innovative university that strengthens the Eastern Switzerland region with forward-looking initiatives and makes a significant contribution to its economic and social development. For more information about *OST*, please refer to http://www.ost.ch.

About SFTI

SFTI (Swiss Fintech Innovations) is an independent association of Swiss financial institutions committed to drive collaboration and digital innovations in the financial services industry. For more information about *SFTI*, please refer to http://www.sfti.ch.

Content

Management Summary

The integration of Artificial Intelligence (AI) into the Swiss financial sector is reshaping operational landscapes, offering significant enhancements in efficiency, compliance, and strategic decision-making. This white paper, titled "Development of a Scalable Framework for Implementing Artificial Intelligence in Swiss Financial Institutions," aims to create a comprehensive framework tailored to the unique regulatory and operational environment of Swiss financial institutions. Lead by OST (Eastern Switzerland University of Applied Sciences), Institute for Finance & Law, in cooperation with SFTI (Swiss FinTech Innovations), the study focuses on developing a practical and scalable AI framework applicable across various functions, including, for example, compliance and risk management.

Objectives and Approach

The primary objective of this study is to facilitate the adoption of AI across different functions within Swiss financial institutions. The framework addresses key success factors for AI implementation, ensuring alignment with regulatory requirements and organizational goals while delivering measurable benefits and satisfying involved stakeholders' needs. Specific objectives include ensuring regulatory alignment with stringent Swiss requirements, integrating AI strategies with organizational goals to enhance efficiencies, and developing strategies for scalable AI implementations.

The study employs a mixed-methods approach, leveraging insights from a comprehensive survey conducted among SFTI members. This survey gathered input on practical AI applications within compliance and other operational functions (excluding client advisory), focusing on decision-making approaches, implementation models, success factors, and challenges encountered. Notably, 24% of the AI use cases were related to compliance areas; however, this differentiation is not deemed critical for the framework's application across various functions.

Key Findings

1. **Decision-Making Approaches**: Institutions employ structured frameworks for identifying high-value use cases, often starting with proof-of-concept (PoC) validations to assess feasibility and potential ROI. 37.5% of institutions use AI-specific decision-making approaches, the majority treats AI projects like other IT or business initiatives.
2. **Implementation Models**: A phased approach is common, involving stages from discovery to full deployment. Agile methodologies are frequently used to ensure flexibility and adaptability. The majority of institutions (87.5%) implements AI projects like other IT or business initiatives, relying on existing implementation models.
3. **Success Factors**: Strategic alignment with business goals and robust internal capabilities are critical. Governance frameworks ensure compliance with regulatory standards. Key success factors are “Strategic Alignment” (67%), “Invest in Internal Capabilities” (67%) and “Implement Robust Governance Frameworks” (50%).
4. **Challenges**: Knowledge gaps remain a significant barrier, alongside privacy concerns and regulatory complexities. Cultural resistance and integration with legacy systems also pose challenges. Key challenges are “Knowledge & Expertise” (50%), “Privacy, Security & Data Usage Issues” (33%), “Regulatory & Compliance Issues” (33%) and “Cultural & Organizational Challenges” (33%).

Scalability and Recommendations

The proposed framework is inherently scalable, allowing institutions to expand their AI initiatives efficiently without requiring structural changes. By leveraging best practices such as incremental scaling, modular architectures, and continuous monitoring, financial institutions can unlock the full potential of AI technologies across their operations.

The framework is structured into six key elements with 33 logical components – the "what" – each accompanied by a total of 105 clear, step-by-step instructions – the "how" – outlining the necessary actions, pertinent questions, and desired outcomes. While certain steps may appear repetitive across different elements and components of the framework, this repetition underscores their significance: Some steps might be optional in one context but mandatory in another, highlighting their critical role in the overall implementation process.

Key recommendations include aligning AI initiatives with strategic business objectives, investing in internal capabilities through targeted training programs, establishing robust governance frameworks, prioritizing data quality and privacy, addressing cultural resistance through change management strategies, adopting a phased implementation approach, continuously monitoring performance metrics, and proactively mitigating risks associated with AI adoption.

Conclusion

This study provides a robust foundation for understanding how AI can be implemented effectively within Swiss financial institutions while addressing regulatory requirements and operational challenges. By combining insights from industry practitioners with rigorous analysis of real-world use cases, it offers a practical roadmap for leveraging AI as a transformative tool in finance. The findings will guide the development of a scalable AI framework tailored to the unique needs of the Swiss financial sector.

Acknowledgment

We extend our heartfelt gratitude to all the individuals and organizations who contributed to the survey and study report. Your insights, expertise, and willingness to share your knowledge have been invaluable to the success of this study.

In particular, we wish to thank Tiphanie Bent, André Bodmer, Remo Brechbühl, Jennifer Chang, Francisco Merlos Fernández, Katharina Fulterer, Julinda Gllavata, Christian Hormann, Andreas Knaus, Ante Plazibat, André Renfer, Andreas Rickli, Philipp Rosenauer, Samuel Scheidegger, Oliver Schneider, and Christian Sebregondi for their time, guidance, and thoughtful responses, which have significantly enriched the findings presented here. Your contributions have provided essential perspectives that greatly enhance the value and relevance of this work.

Thank you for your support and engagement!

1. Introduction and Study Approach

The rapid integration of Artificial Intelligence (AI) into the financial services sector is reshaping how institutions operate, offering transformative improvements in efficiency, compliance, and decision-making. Swiss financial institutions, operating within a highly regulated and data-sensitive environment, are uniquely positioned to benefit from AI technologies. However, the adoption of AI also presents challenges that require a tailored approach to ensure alignment with regulatory requirements, organizational goals, and operational realities incl. technological setup.

This study, titled *"Development of a Scalable Framework for Implementing Artificial Intelligence in Swiss Financial Institutions,"* was initiated by SFTI (Swiss FinTech Innovations) and co-conducted with OST (Eastern Switzerland University of Applied Sciences, Institute for Finance & Law) to address these challenges. It aims to develop a comprehensive framework that supports the effective adoption of AI across various functions, including compliance, risk management, and customer service. The framework is designed to be practical, scalable, and adaptable to the unique needs of Swiss financial institutions.

1.1 Study Objectives

The primary objective of this study is to provide Swiss financial institutions with a structured framework for implementing AI technologies effectively and sustainably. This framework addresses key success factors while mitigating challenges associated with AI adoption. Specific objectives include:

1. **Regulatory Alignment:**
   Ensure that AI implementations comply with applicable Swiss regulations relevant for financial institutions, such as AML (Anti-Money Laundering), KYC (Know Your Customer), GDPR (General Data Protection Regulation), the Federal Data Protection Act (FADP), and FINMA Guidance 08/2024.
2. **Organizational Integration:**
   Align AI strategies with organizational goals to enhance operational efficiencies while fostering cultural readiness for technological transformation and AI adoption.
3. **Scalability:**
   Develop strategies for scaling AI implementations across various functions, ensuring that the framework remains adaptable as institutions expand their use of AI.
4. **Practical Application:**
   Provide actionable insights into decision-making approaches, implementation models, success factors, and challenges encountered during AI adoption.

1.2 Study Methodology

The study leverages a mixed-methods approach to ensure comprehensive insights into AI adoption within Swiss financial institutions:

1. **Survey Insights:**
   A survey was distributed to 12 Sounding Board members representing six SFTI member companies to gather input on practical AI applications within compliance and other operational functions (excluding client advisory). The survey achieved a 100% response rate from Sounding Board members and included additional input from two member companies, totaling responses from eight SFTI member institutions.
   - **Focus Areas:**
     - Examples of AI use cases in compliance and non-compliance functions.
     - Decision-making approaches and implementation models.
     - Key success factors and challenges encountered during implementation.

2. **Analysis of Use Cases:**
   The study analyzed 21 reported use cases to identify trends in decision-making models, implementation approaches, success factors, and challenges. These insights form the foundation for developing a scalable framework tailored to the needs of Swiss financial institutions.
3. **Expert Collaboration:**
   The study draws on expertise from industry practitioners and academic partners to ensure that the framework reflects both practical realities and theoretical rigor.

1.3 Report Structure

This report is organized into the following chapters:

1. **Management Summary**
   A concise overview of the study's objectives, key findings, and recommendations.
2. **Introduction and Study Approach**
   An introduction to the study's purpose, objectives, methodology, and structure.
3. **AI in Financial Services – Key Drivers and Regulatory Overview**
   An exploration of the drivers behind AI adoption in financial services and an overview of relevant regulatory frameworks in Switzerland.
4. **Application of AI in the Swiss Financial Industry – Analysis of Use Cases**
   A detailed analysis of selected AI use cases reported by SFTI members, focusing on decision-making approaches, implementation models, success factors, and challenges.
5. **Framework for Implementing AI in Swiss Financial Institutions**
   A comprehensive framework outlining the key elements required for successful AI implementation.
6. **Scalability of the Framework**
   A discussion on how the proposed framework supports scalability without requiring structural changes.
7. **Conclusion and Recommendations**
   Final observations on the findings and actionable recommendations for Swiss financial institutions adopting AI technologies.

This study provides a robust foundation for understanding how AI can be implemented effectively within Swiss financial institutions while addressing regulatory requirements and operational challenges. By combining insights from industry practitioners with rigorous analysis of real-world use cases, it offers a practical roadmap for leveraging AI as a transformative tool in finance.

2. AI in Financial Services – Key Drivers and Regulatory Overview

2.1 Drivers of AI in Financial Services

In the contemporary landscape of technological advancement, Artificial Intelligence (AI) stands out as a pivotal force reshaping industries across the globe. Its transformative potential is particularly evident in financial services, where AI not only enhances operational efficiencies but also addresses stringent compliance demands. This chapter explores the key drivers propelling AI adoption both generally and specifically within the realms of financial services and compliance.

2.1.1 General Drivers of AI

The ascent of AI can be attributed to several overarching factors that collectively fuel its integration into various sectors. At the forefront is the **technological advancement** that has significantly increased computational power and data processing capabilities. This progress has enabled the development of sophisticated algorithms capable of performing complex tasks with remarkable efficiency.

Another critical driver is the **availability of data**. The digital age has ushered in an era characterized by vast amounts of data generation, providing a rich resource for training AI models. This abundance allows AI systems to learn from diverse datasets, enhancing their predictive accuracy and decision-making capabilities.

Moreover, AI offers substantial **cost efficiency** by automating repetitive tasks traditionally performed by humans. This automation not only reduces operational costs but also frees up human resources for more strategic roles, thereby improving overall productivity. Additionally, AI's ability to provide advanced analytics supports **enhanced decision-making**, enabling organizations to make informed choices based on data-driven insights.

2.1.2 Drivers of AI in Financial Services

Within the financial services sector, AI adoption is driven by several industry-specific factors. **Regulatory pressure** is a significant catalyst, as financial institutions are required to comply with increasingly complex regulatory frameworks. AI tools streamline compliance processes by automating checks and generating accurate reports, thereby reducing the burden on compliance teams.

The sector also benefits from AI's capabilities in **risk management**. By analyzing large datasets, AI systems can identify potential risks more effectively than traditional methods, allowing institutions to mitigate threats proactively. Furthermore, evolving **customer expectations** for personalized and efficient services drive financial institutions to leverage AI for enhancing customer experiences through tailored product offerings and rapid service delivery.

AI's role in **fraud detection** is another compelling driver. Its pattern recognition capabilities enable real-time detection of fraudulent activities, safeguarding institutions from financial losses and reputational damage.

2.1.3 Drivers of AI in Financial Compliance

In the realm of financial compliance, AI's impact is profound due to its ability to enhance **efficiency in compliance operations**. By automating routine tasks such as transaction monitoring and document verification, AI allows compliance teams to focus on more complex issues.

AI systems also offer **adaptability to regulatory changes**, a critical feature given the dynamic nature of financial regulations. These systems can quickly adjust algorithms to comply with new rules, ensuring continuous adherence to regulatory standards. Additionally, as compliance increasingly involves managing sensitive data, AI helps ensure **data security and privacy** through advanced encryption and anomaly detection techniques.

Finally, the rise of **Regulatory Technology (RegTech)** driven by AI provides innovative solutions for compliance challenges. RegTech enables institutions to stay ahead in a competitive landscape by offering tools that streamline compliance processes and reduce costs.

In conclusion, the drivers of AI adoption are multifaceted and interwoven with technological advancements and industry-specific needs. In financial services and compliance, these drivers underscore AI's potential to transform operations by enhancing efficiency, meeting regulatory demands more effectively, and delivering superior customer experiences.

2.2 Regulatory Overview of AI in Financial Services

The regulatory landscape for Artificial Intelligence (AI) in Switzerland continues to evolve as AI technologies become integral to financial services, particularly in compliance-related functions such as **Anti-Money Laundering (AML)** and **Know Your Customer (KYC)**. Switzerland's regulatory approach is characterized by its principle-based, **technology-neutral framework**, which allows existing laws to govern new technologies while fostering innovation and ensuring alignment with international standards. This chapter provides an up-to-date overview of the regulatory framework for AI in Switzerland, incorporating the latest developments outlined in FINMA Guidance 08/2024.

2.2.1 General AI Regulation in Switzerland

Switzerland's regulatory approach to AI remains grounded in its **technology-neutral legal framework**. Instead of enacting dedicated AI-specific legislation, Switzerland applies existing laws to emerging technologies. The **Federal Data Protection Act (FADP)**, which came into force in September 2023, remains a cornerstone of AI governance in Switzerland. This law emphasizes transparency, data minimization, and the protection of individuals' rights, including the right to understand how their personal information is processed by AI systems.

With the publication of **FINMA Guidance 08/2024**, Swiss financial institutions now face enhanced expectations for managing AI-related risks. These include maintaining comprehensive inventories of AI systems, conducting rigorous risk assessments, and ensuring robust governance, transparency, and accountability frameworks. The supervisory authority's guidance reflects the **growing complexity of AI technologies** and the need for institutions to **adapt their governance structures** accordingly.

Switzerland's alignment with international standards, particularly the **EU AI Act**, remains a strategic priority. The **Swiss Federal Council** continues to evaluate the compatibility of Swiss regulatory practices with emerging global frameworks, ensuring that Swiss financial institutions are well-positioned to meet cross-border compliance expectations. This alignment includes fostering transparency, mitigating biases, and implementing proactive governance measures for AI systems deployed in high-risk areas. In November 2023, the Swiss Federal Council has instructed the **Federal Department of Environment, Transport, Energy and Communications (DETEC)** to identify potential approaches to regulating AI. This analysis is expected to be published in early 2025 and shall serve as the basis to issue a concrete mandate for an AI regulatory proposal in 2025 and clarify areas of responsibility.

2.2.2 AI Regulation in Financial Services

Within the financial services sector, the **Swiss Financial Market Supervisory Authority (FINMA)** plays a pivotal role in overseeing AI applications. Although FINMA does not regulate AI technologies directly, its **updated supervisory guidance** emphasizes the critical need for robust governance, risk management, and compliance frameworks to ensure that AI systems operate ethically and transparently.

While **FINMA's Guidance 08/2024** does not constitute formal regulation of AI applications in the financial industry, it represents the Swiss supervisor's current level of thinking in the field and is

closely scrutinized and typically adhered to by supervised institutions. Emphasizing a risk-based approach, the guidance outlines expectations based on the scale and impact of AI applications and as a consequence might call supervised institutions to consider to **maintain centralized inventories** of all AI applications, detailing their purpose, risk profiles, and performance metrics, to **align risk management frameworks** to address operational, IT, and legal risks associated with AI deployment, and to **establish mechanisms to ensure the explainability** of AI-driven decisions, particularly in high-stakes applications such as AML, fraud detection, and credit scoring. By adhering to these expectations, institutions can better align their AI initiatives with FINMA's supervisory priorities, ensuring both compliance and operational resilience.

The **emphasis on transparency and accountability** aligns with both Swiss data protection laws and international standards, such as the EU AI Act. These frameworks collectively underscore the importance of mitigating risks while leveraging AI's potential to enhance efficiency and accuracy in financial services.

2.2.3 Specific Regulatory Considerations for Financial Compliance

In compliance functions like AML and KYC, AI technologies are widely used to streamline processes and improve accuracy. However, their deployment introduces challenges related to data privacy, transparency, and the potential for algorithmic bias. FINMA's Guidance 08/2024 reinforces the need for institutions to **conduct regular monitoring activities** to identify and mitigate biases in AI systems, to ensure that **data governance frameworks** safeguard the integrity, accuracy, and representativeness of data, and to provide **mechanisms for individuals to challenge automated decisions** and request human intervention where necessary.

As mentioned, these expectations align with the principles set out in the EU AI Act, which categorizes AI systems based on their potential risks and imposes stricter regulations on high-risk applications. Institutions operating across jurisdictions must align their compliance frameworks with these evolving regulatory expectations – at home and abroad - to avoid penalties and maintain trust.

2.2.4 Impact on the Use of AI in Financial Services

The regulatory environment significantly shapes the deployment of AI technologies in financial services, particularly in high-risk areas such as AML and KYC. Key regulatory impacts include:

1. **Enhanced Compliance Requirements:** Institutions must ensure that their AI systems comply with both Swiss and international standards, addressing requirements for transparency, accountability, and data protection.
2. **Focus on Transparency:** AI-driven decisions must be explainable to regulators, customers, and other stakeholders, fostering trust and accountability.
3. **Risk Management:** AI systems must be integrated into robust risk management frameworks that address potential biases and ensure the fair treatment of all customers.
4. **Innovation within Regulatory Boundaries:** Regulations provide clear guidelines for responsible AI use, enabling institutions to innovate while ensuring compliance and consumer protection.

2.3 FINMA's Perspectives on Risks Imposed by AI in Finance

The **Swiss Financial Market Supervisory Authority (FINMA)** continues to play a pivotal role in ensuring that financial institutions integrate advanced technologies like **Artificial Intelligence (AI)** within a secure and transparent framework. In alignment with its principle-based, technology-neutral regulatory approach, FINMA has elaborated on the risks posed by AI and recommended robust governance and risk management measures, appropriate and relative to the risks imposed. This chapter synthesizes key elements both from **FINMA's Risk Monitor 2023** and the recently published **FINMA Guidance 08/2024** to reflect the most current regulatory expectations.

2.3.1 Key Risks Identified by FINMA

Governance and Accountability: FINMA emphasizes that the use of AI introduces complex governance challenges, particularly regarding accountability. Supervised institutions must ensure clear lines of responsibility for AI applications, including those outsourced to third parties. The decentralized development of AI within organizations can hinder consistency in standards and oversight. To address this, FINMA now explicitly expects institutions to maintain a centrally managed inventory of AI applications, accompanied by a robust risk classification framework. This inventory should detail the purpose, data usage, testing processes, and potential risks associated with each AI system.

Furthermore, institutions must establish clear accountability mechanisms for AI deployment and operation. These mechanisms should define responsibilities across the lifecycle of AI applications, from development to monitoring, and ensure that human operators retain ultimate oversight and decision-making authority.

Risk Classification and Inventory Management: A recurring concern highlighted by FINMA is the inconsistent definition and classification of AI applications across institutions. Some institutions have narrowly defined AI, leading to incomplete inventories and risk assessments. Different to the EU AI Act, FINMA does not designate specific AI applications as "high-risk" but leaves this determination to supervised institutions, following respective review activities if necessary. FINMA Guidance 08/2024 underscores the necessity of a broad and consistent definition of AI, incorporating both traditional and generative AI systems. Institutions must establish comprehensive criteria to identify and categorize AI applications, focusing on materiality and risk exposure, including their potential for regulatory non-compliance or reputational harm.

Data Quality and Model Robustness: The quality of data used in AI applications remains a cornerstone of their reliability and compliance. FINMA's supervisory observations reveal that many institutions lack stringent controls to ensure the integrity, accuracy, and representativeness of data. Historical biases in training datasets and the use of unstructured or manipulated data pose significant risks. Institutions are now required to implement robust data governance frameworks that include comprehensive documentation of data sources, regular quality checks for completeness, accuracy, and appropriateness, and mechanisms to monitor and mitigate data drift.

For model robustness, FINMA advocates for rigorous testing and monitoring, including stress tests, sensitivity analyses, and validation against predefined performance indicators. Continuous model updates are necessary to adapt to changing market conditions and emerging risks.

Explainability and Transparency: AI's complexity often leads to challenges in understanding and explaining model decisions. FINMA emphasizes that explainability is critical for trust and accountability. Institutions must ensure that AI-driven outcomes are interpretable and can be communicated effectively to stakeholders, including customers, auditors, and regulators. Documentation should include detailed explanations of model logic, assumptions, and limitations, as well as fallback solutions for handling erroneous or unexpected outcomes.

Independent Review and Oversight: A key addition in FINMA Guidance 08/2024 is the requirement for independent reviews of AI systems, if applicable. These reviews should assess the appropriateness, reliability, and compliance of AI applications, with results incorporated into the decision-making process. Institutions must ensure that reviewers possess the necessary expertise and independence from the development teams.

Operational and Outsourcing Risks: As institutions increasingly rely on third-party providers for AI solutions, FINMA identifies significant operational and outsourcing risks. Institutions must implement robust due diligence processes for external vendors, ensuring that providers adhere to the same governance and data standards expected internally. Contractual agreements should clearly delineate responsibilities and liabilities, and additional controls should be established to monitor outsourced AI applications.

Addressing Discrimination and Fairness: Bias in AI models can lead to discriminatory outcomes, particularly in areas like credit scoring and customer profiling. FINMA's updated guidance mandates ongoing monitoring of AI systems to detect and mitigate biases. Institutions are expected to incorporate fairness metrics into their testing frameworks and ensure compliance with ethical standards to avoid unjustified discrimination.

Continuous Monitoring and Adaptation: Given the dynamic nature of AI technologies, FINMA stresses the importance of continuous monitoring and adaptation. Institutions must establish performance benchmarks and validation thresholds for AI systems, monitor input data changes to identify and address data drift, and document and analyze instances of manual intervention or overrides to identify systemic issues.

2.3.2 Key Implications for Swiss Financial Institutions

While FINMA's updated regulatory guidance does not constitute formal regulation of AI applications in the financial industry it imposes clear expectations on supervised institutions. Based on the scale and impact of their AI applications they might be required to:

1. **Develop Holistic AI Risk Management Frameworks:** Institutions must maintain centralized AI inventories with detailed documentation of purpose, data usage, and associated risks. Additionally, risk assessments must align with FINMA's enhanced classification criteria for both traditional and generative AI systems.
2. **Strengthen Human Oversight Mechanisms:** Despite AI's growing autonomy, institutions must ensure robust human oversight. This includes assigning accountability throughout the AI lifecycle, from design and deployment to ongoing operations, ensuring decision-making processes remain transparent and trustworthy.
3. **Enhance Compliance and Transparency:** Institutions need to align AI operations with FINMA's principles, emphasizing explainability, fairness, and reliability. This involves fostering internal policies that reflect Swiss and international regulatory standards, including provisions for addressing potential biases in AI outputs.
4. **Invest in Independent Reviews and Expertise:** Institutions should integrate independent reviews into their risk management processes. Upskilling employees and collaborating with external experts ensures that organizations remain equipped to manage the evolving complexities of AI technologies.
5. **Implement Scalable Governance Structures:** FINMA underscores the importance of scalable governance frameworks that can adapt to the evolving scope and complexity of AI applications. These structures must include clear accountability for outsourced solutions and mechanisms for monitoring compliance across all operational levels.
6. **Foster Resilience Through Continuous Monitoring:** Institutions must establish dynamic systems to track AI performance, ensuring prompt identification and mitigation of risks such as data drift, model degradation, or emerging vulnerabilities. Regular stress testing and adaptation processes will be essential for maintaining system reliability.

The risks identified by FINMA underscore the complexity of implementing AI technologies in the financial sector. While AI holds the potential to revolutionize financial services by enhancing operational efficiency and decision-making accuracy, it also presents new challenges that financial institutions must manage carefully. By adhering to FINMA's updated guidelines, Swiss financial institutions can responsibly integrate AI technologies, balancing innovation with risk management and regulatory compliance. This approach not only enhances operational efficiency but also reinforces the trust and integrity of the Swiss financial sector.

2.4 Impact of the EU Artificial Intelligence Act (AI Act) on Switzerland's Financial Services and Compliance

The **European Union's Artificial Intelligence Act (AI Act)** represents a groundbreaking regulatory initiative aimed at ensuring the safe, ethical, and transparent use of AI technologies across industries. While primarily an EU regulation, its **extraterritorial scope** significantly impacts non-EU entities, including Swiss financial institutions serving EU clients or utilizing AI systems affecting EU residents. The recent FINMA Guidance 08/2024 complements these developments by providing specific guidance for Swiss institutions to align with evolving international standards.

2.4.1 Key Elements of the EU AI Act and Its Alignment with FINMA's Expectations

The **EU AI Act** adopts a **risk-based approach** to the regulation of AI systems, categorizing them into four distinct levels based on the potential risks they pose to safety and fundamental rights (see Figure 1):

1. **Unacceptable risk** – These AI systems, which may pose serious threats to safety and rights, are banned.
2. **High risk** – AI systems in sectors like finance, including **credit scoring**, **AML**, and **KYC**, fall under this category and are subject to stringent oversight. They must pass **conformity assessments**, provide **explainability**, and have **human oversight**.
3. **Limited risk** – These systems face moderate transparency requirements, including informing users of AI's involvement.
4. **Minimal risk** – No additional requirements apply to these systems, as their use is deemed safe.

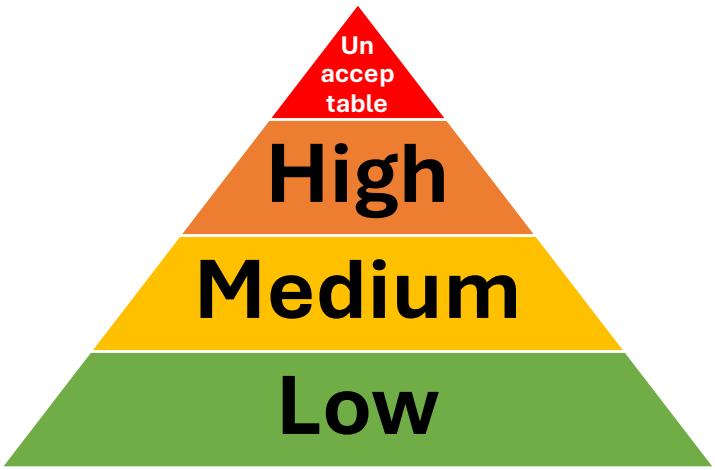


Figure 1: Risk Classification in EU AI Act

Consequently, **high-risk AI applications**, such as those used in **financial compliance** (e.g., Anti-Money Laundering [AML] and Know Your Customer [KYC]), are subject to stringent oversight, including conformity assessments, explainability requirements, and mandatory human oversight. While FINMA refrains from explicitly designating specific AI applications as "high risk," leaving this determination to supervised institutions following respective review, the outlined requirements of the EU AI Act align closely with FINMA's updated expectations in Guidance 08/2024, emphasizing the importance of centralized inventories, thorough risk classification, and robust governance mechanisms for AI systems.

2.4.2 Extraterritorial Application and Compliance Challenges for Swiss Institutions

The European Union's AI Act introduces extraterritorial provisions that extend its influence far beyond EU borders, impacting Swiss financial institutions that interact with EU citizens, serve EU markets, or utilize AI systems with a material effect within the EU. This regulatory scope compels Swiss

institutions to align their AI operations with the Act's stringent requirements, addressing challenges that go beyond domestic regulatory obligations. To comply effectively, Swiss financial institutions must prioritize several key aspects:

Transparency and Documentation: Transparency lies at the heart of the AI Act's requirements. Institutions must ensure that their AI systems provide clear, human-readable explanations for decisions, particularly in sensitive areas like credit scoring, fraud detection, or investment advice. This involves implementing **robust documentation processes** that detail (i) the purpose, logic, and operation of AI models, (ii) data inputs, training methodologies, and potential limitations, and (iii) mechanisms to explain decisions to non-technical stakeholders, including customers, regulators, and auditors. Such transparency is critical not only for regulatory compliance but also for fostering trust among clients and mitigating reputational risks. Swiss institutions should consider adopting tools and frameworks that enable the **systematic documentation and review of AI systems**.

Risk Management and Monitoring: AI systems are inherently dynamic, making continuous monitoring and post-market surveillance essential to maintaining their integrity and performance. The AI Act mandates proactive risk management practices to address: (i) **Model Drift:** Monitoring for deviations in AI behavior as input data evolves over time, (ii) **Bias:** Detecting and mitigating biases that may result in unfair or discriminatory outcomes, and (iii) **Robustness:** Ensuring that AI systems remain reliable across varying conditions and unexpected scenarios. Swiss institutions must establish **comprehensive monitoring frameworks** that leverage advanced analytics and automated alert mechanisms to detect potential issues in real time. Additionally, FINMA's complementary guidance in Guidance 08/2024 emphasizes the importance of integrating these practices into centralized governance structures to enhance consistency and efficiency.

Human Oversight: Despite the increasing sophistication of AI systems, the AI Act underscores the necessity of **maintaining human involvement in critical decision-making processes**. Institutions must design their governance frameworks to ensure that (i) human operators retain **accountability** for AI-driven decisions, (ii) AI outputs are subject to **human validation**, particularly in high-stakes scenarios such as loan approvals or regulatory compliance reviews, and (iii) clear **escalation paths** are established for addressing unexpected outcomes or ethical concerns. By embedding human oversight into the lifecycle of AI applications, institutions can mitigate the risks of over-reliance on AI and safeguard against errors or unintended consequences.

Integration into Swiss Governance Frameworks: The requirements outlined in the AI Act align closely with FINMA's expectations for Swiss financial institutions. FINMA's Guidance 08/2024 reinforces the need for Swiss institutions to integrate transparency, monitoring, and human oversight into their governance structures. Institutions are encouraged to (i) maintain **centralized inventories** of AI systems, detailing their purposes, risks, and compliance measures, (ii) conduct **regular risk assessments** that incorporate the unique challenges posed by cross-border operations, and (iii) **collaborate** with both Swiss and EU regulators to ensure alignment and clarify compliance expectations.

Strategic Alignment and Operational Resilience: For Swiss financial institutions, addressing these extraterritorial challenges is not merely a compliance exercise but an opportunity to enhance operational resilience and strategic positioning. Institutions that successfully integrate these requirements into their operations are able to build stronger customer trust by demonstrating ethical and transparent AI practices, **leverage robust governance frameworks** to adapt more easily to future regulatory changes, and strengthen their competitive edge in both domestic and international markets by showcasing leadership in responsible AI adoption.

In summary, the extraterritorial provisions of the AI Act present both challenges and opportunities for Swiss financial institutions. By aligning with the Act's requirements and FINMA's complementary guidance, institutions can navigate these complexities effectively, ensuring compliance while enhancing their capacity to innovate and operate in a rapidly evolving regulatory environment.

2.4.3 Operational Adjustments and Strategic Realignments

To meet the dual demands of the EU AI Act and FINMA's updated supervisory expectations, Swiss financial institutions must embark on significant operational adjustments and strategic realignments. These efforts are essential not only for compliance but also for enhancing organizational resilience and readiness in a rapidly evolving regulatory landscape. Institutions must focus on three critical areas:

Developing Comprehensive AI Inventories: A cornerstone of both the EU AI Act and FINMA Guidance 08/2024 is the requirement for a detailed inventory of AI systems. This inventory serves as a centralized repository for documenting all AI applications within an institution, covering:

- **Purpose:** Clearly defined use cases for each AI system, whether for fraud detection, risk assessment, or customer profiling.
- **Risk Profiles:** Detailed analyses of potential operational, reputational, and compliance risks associated with each application.
- **Performance Metrics:** Ongoing documentation of key performance indicators (KPIs) to track model accuracy, reliability, and fairness over time.

Institutions must implement robust processes to keep these inventories up to date, ensuring that new applications are seamlessly integrated, and risks are systematically assessed. This practice not only supports compliance but also facilitates transparency and informed decision-making.

Aligning Risk Management Frameworks: AI introduces unique risks that extend beyond traditional operational and IT concerns, requiring institutions to enhance their existing risk management frameworks. These frameworks should address:

- **Operational Risks:** Including the potential for model failure, data inaccuracies, or integration issues with legacy systems.
- **IT Risks:** Such as vulnerabilities in AI infrastructure, cybersecurity threats, and system downtime.
- **Legal Risks:** Encompassing compliance with evolving regulatory requirements and potential liabilities arising from AI-driven decisions.

To mitigate these risks, institutions should adopt a holistic approach, incorporating regular risk assessments, stress testing, and validation procedures. Alignment with FINMA's recommendations on centralized governance ensures that these measures are consistently applied across all AI systems.

Adopting Scalable and Adaptive Solutions: Scalability is essential for ensuring that AI initiatives can grow without compromising compliance or operational stability. Modular architectures and adaptive frameworks enable institutions to:

- **Seamlessly Integrate New Use Cases:** By leveraging reusable components and APIs, institutions can efficiently expand their AI capabilities.
- **Maintain Compliance at Scale:** Adaptive frameworks allow for the incorporation of new regulatory requirements without overhauling existing systems.
- **Enhance Flexibility:** Modular solutions make it easier to adapt AI applications to evolving business needs and technological advancements.

Institutions should also invest in advanced monitoring tools and automation to manage scalability effectively, ensuring that performance, reliability, and compliance are maintained as AI systems expand.

Strategic Realignments for Long-Term Success: Operational adjustments must be complemented by broader strategic realignments to embed AI compliance and governance into the institution's core philosophy. This includes:

- **Fostering a Compliance-First Culture:** Encouraging proactive engagement with regulatory requirements and promoting accountability across all levels of the organization.
- **Upskilling Workforce:** Ensuring employees have the expertise to manage and operate AI systems responsibly, aligning with FINMA's emphasis on human oversight and independent reviews.
- **Collaborating with Stakeholders:** Engaging regulators, technology providers, and academic partners to ensure alignment with best practices and access to cutting-edge solutions.

By implementing these operational adjustments and strategic realignments, Swiss financial institutions can navigate the complexities of AI adoption while maintaining compliance and strengthening their competitive positioning. These efforts not only address immediate regulatory challenges but also lay the groundwork for sustainable innovation and growth in the digital era.

2.4.4 Implications for Swiss Financial Institutions

The integration of FINMA's updated supervisory expectations and the stringent requirements of the EU AI Act presents a transformative challenge for Swiss financial institutions. Successfully navigating this convergence requires proactive measures that address compliance, operational adjustments, and strategic alignment. By doing so, institutions can not only meet regulatory expectations but also position themselves as leaders in ethical and innovative AI adoption.

Cross-Border Compliance – Bridging Swiss and EU Regulatory Standards: The dual demands of Swiss and EU regulations necessitate meticulous alignment to ensure AI systems operate seamlessly across jurisdictions. Swiss institutions must implement robust mechanisms to guarantee:

- **Regulatory Consistency:** AI systems should adhere to Swiss principles, such as those outlined in FINMA Guidance 08/2024, while simultaneously meeting EU requirements for transparency, risk management, and data protection.
- **Avoidance of Penalties:** Preemptive compliance reduces the risk of sanctions or operational disruptions stemming from regulatory breaches in either jurisdiction.
- **Operational Resilience:** Cross-border compliance frameworks must be agile enough to adapt to evolving regulatory landscapes, ensuring sustained functionality and reliability.

Prioritizing Explainability and Fairness: The ethical use of AI is central to both FINMA's and the AI Act's frameworks. In order to strengthen regulatory compliance and support long-term trust in AI-driven operations, institutions must focus on designing systems that:

- **Promote Explainability:** AI decisions, particularly those affecting customers—such as credit approvals or investment recommendations—must be transparent and interpretable. This ensures that decisions can be explained in clear, non-technical terms to customers, regulators, and other stakeholders.
- **Mitigate Biases:** By incorporating fairness metrics and conducting regular audits, institutions can identify and address potential biases in AI systems, ensuring equitable outcomes across demographic groups.
- **Foster Trust:** Transparent and fair AI systems enhance stakeholder confidence, reinforcing the institution's reputation for ethical practices.

Enhanced Collaboration with Regulators: Proactive and sustained engagement with regulators is essential for ensuring that AI initiatives align with both FINMA's supervisory expectations and the EU AI Act. This collaboration involves:

- **Clarifying Obligations:** Institutions should actively seek guidance on ambiguous compliance requirements, reducing uncertainty and fostering mutual understanding with regulators.
- **Demonstrating Commitment:** Regularly sharing progress on AI compliance initiatives signals a proactive stance, helping institutions build positive relationships with supervisory authorities.
- **Leveraging Insights:** Participation in regulatory discussions allows institutions to anticipate upcoming changes and adapt their strategies accordingly.

Strategic Positioning in a Global Market: By aligning with these regulatory frameworks, Swiss financial institutions can achieve significant competitive advantages, including:

- **Enhanced Transparency:** Clear documentation and communication of AI processes not only meet regulatory demands but also attract clients who value ethical and transparent financial services.
- **Risk Mitigation:** Comprehensive compliance frameworks reduce the likelihood of reputational and operational risks associated with AI adoption.
- **Leadership in Innovation:** Institutions that embrace these frameworks are well-positioned to lead the global financial services market, leveraging AI to deliver innovative and trustworthy solutions.

In conclusion, the convergence of FINMA's updated expectations and the EU AI Act requires Swiss financial institutions to adopt a comprehensive and proactive approach. By prioritizing cross-border compliance, ethical AI use, and collaborative regulatory engagement, institutions can not only meet these challenges but also capitalize on opportunities to strengthen their market positioning and drive sustainable growth.

Penalties for Non-Compliance with EU AI Act

The **EU AI Act** sets out significant penalties for non-compliance, which can impact both EU-based and non-EU entities, including **Swiss financial service providers** that operate in the EU market or affect EU residents with their AI systems.

1. **Fines for High-Risk and Prohibited AI Systems:**
   - For non-compliance with the provisions on **high-risk AI systems** (e.g., AI used in **AML/KYC** functions or credit scoring), penalties can reach **up to €20 million or 4% of the company's total worldwide annual turnover**, whichever is higher. This applies if the AI system is deployed without undergoing the necessary **conformity assessments** or without adhering to mandatory transparency and risk management requirements (EU AI Act, Article 71).
   - Using **prohibited AI systems** (those classified under the "unacceptable risk" category, such as systems that violate fundamental rights) can also result in the same financial penalties.
2. **Failure to Cooperate with Authorities:**
   - Companies, including Swiss financial institutions, that fail to cooperate with EU regulatory authorities or fail to provide required information during investigations may face penalties of **up to €10 million or 2% of their worldwide annual turnover**, depending on the nature of the violation (Article 71, EU AI Act).
3. **Incorrect or Misleading Information:**
   - Providing false or misleading information during the conformity assessment or regulatory review process can result in fines **up to €10 million or 2% of worldwide turnover**.

Implications for Swiss Financial Service Providers

- Swiss financial service providers, particularly those offering **cross-border services** or utilizing AI technologies that influence EU citizens, must ensure full compliance with the EU AI Act's requirements for high-risk systems, such as AML and KYC tools. Non-compliance with these provisions will subject them to the same penalties as EU-based entities, which can be financially devastating given the significant turnover-based fines.
- Given the **extraterritorial scope** of the AI Act (Article 2), even AI systems developed and deployed in Switzerland but affecting individuals or businesses within the EU fall under the Act's purview. Therefore, Swiss financial institutions must ensure that their AI systems undergo the necessary conformity assessments and adhere to transparency, explainability, and human oversight standards to avoid such penalties.
- Swiss financial service providers must take **proactive steps** to comply with the EU AI Act, especially when using AI systems classified as high-risk. The potential fines for non-compliance, particularly for failing to meet conformity assessment requirements or deploying prohibited AI systems, are substantial and can reach €20 million or 4% of global turnover, making compliance essential for institutions operating in both Swiss and EU markets.

3. Application of AI in the Swiss Financial Industry – Analysis of AI Use Cases

In recent years, the Swiss financial industry has increasingly embraced artificial intelligence (AI) to enhance operational efficiency, improve compliance, and drive innovation. This chapter provides an in-depth analysis of selected AI use cases within the industry, focusing on both compliance and non-compliance functions. The insights are drawn from a survey conducted with SFTI member companies, which aimed to gather input on decision-making approaches, implementation models, success factors, and challenges encountered. This forms the basis for understanding how AI is being applied across various functions within Swiss financial institutions.

3.1 Survey Overview – Focus Areas and Key Findings

To gather comprehensive data, a survey was conducted among SFTI members, targeting both compliance and other operational functions (and deliberately excluding AI uses cases in client advisory, as these have been part of separate studies and whitepapers). This survey aimed to understand the practical applications of AI, with a focus on decision-making processes, implementation strategies, and the factors influencing success and challenges. The survey achieved a 100% response rate from Sounding Board members and additional input from two member companies, totaling responses from eight SFTI member companies, and providing details on 21 AI use cases implemented by the responding member companies.

3.1.1 Focus Areas

- **AI Use Cases in Compliance vs. Non-Compliance**: The analysis revealed that 24% of AI use cases are related to compliance functions. Despite this differentiation, the framework developed does not distinguish between compliance and non-compliance use cases, as this is not a critical factor for its application (see Figure 2).
- **Decision-Making and Implementation Models**: Insights into how institutions decide on and implement AI projects, including any differences in life-cycle models, were gathered.
- **Key Success Factors and Challenges**: Identification of what drives success and what obstacles are commonly faced in implementing AI solutions.

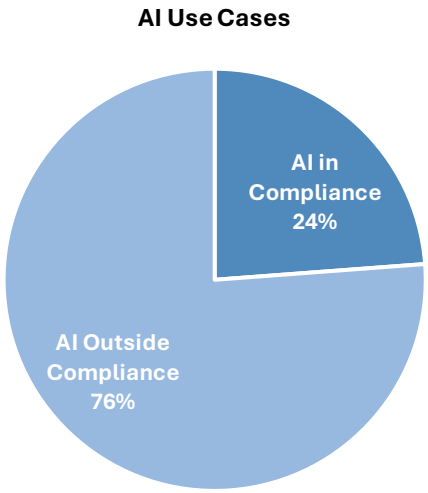


Figure 2: AI Use Cases in Compliance vs. Non-Compliance

3.1.2 Key Findings

- **Decision-Making Approaches**: Institutions employ structured frameworks for identifying high-value use cases, often starting with proof-of-concept (PoC) validations to assess feasibility and potential ROI.
- **Implementation Models**: A phased approach is common, involving stages from discovery to full deployment. Agile methodologies like the Scaled Agile Framework (SAFe) are frequently used to ensure flexibility and adaptability.
- **Success Factors**: Strategic alignment with business goals and robust internal capabilities are critical. Governance frameworks ensure compliance with regulatory standards.
- **Challenges**: Knowledge gaps remain a significant barrier, alongside privacy concerns and regulatory complexities. Cultural resistance and integration with legacy systems also pose challenges.

This underscores the strategic importance of AI in transforming Swiss financial institutions. By understanding decision-making processes, implementation strategies, success factors, and challenges, institutions can better navigate their AI journeys. The insights gained will guide the development of a scalable AI framework tailored to the unique needs of the Swiss financial sector. Detailed findings and recommendations based on these insights are part of the subsequent sections of this report, details of the reported AI use cases can be found in the appendix (see Table 17).

3.2 Findings related to "AI Categories"

The categorization of the 21 AI use cases reported by the SFTI members highlights the history and current trends in leveraging specialized AI technologies within the financial industry. These use cases were classified into three primary categories: **Machine Learning (ML)**, **Generative AI (GenAI)**, and **Large Language Models (LLM)**.[1] The distribution reflects the varying capabilities of these technologies and their alignment with specific task requirements (see Figure 3).

- **Machine Learning ML (67%)**:
  ML dominates the landscape, accounting for **67%** of the use cases. This category is widely applied to tasks requiring structured data analysis, including classification, regression, and anomaly detection. Examples include fraud detection, marketing segmentation, customer identification, and trade surveillance. ML's versatility and proven effectiveness in handling structured datasets make it the backbone of AI applications in finance.
- **Generative AI GenAI (19%)**:
  GenAI is utilized in **19%** of the use cases, particularly where generative capabilities are required. This includes tasks such as summarization, transcription of customer calls, and conversational interfaces like chatbots or AI-driven assistants integrated into productivity tools. Its ability to generate coherent and contextually relevant text makes it ideal for customer-facing or communication-focused applications.
- **Large Language Models LLM (14%)**:
  LLMs are employed in **14%** of the use cases and are preferred for text-heavy tasks. These include sentiment analysis, document processing, and powering advanced conversational agents such as voice- and chatbots. LLMs excel in understanding and generating natural language, making them valuable for applications requiring deep linguistic comprehension.

The breakdown of AI categories demonstrates how financial institutions strategically deploy different AI technologies based on task complexity and data types. Machine Learning remains the most

[1] The category **"Generative AI (GenAI)"** refers to AI applications that generate human-like text and engage in conversational interactions, such as chatbots and virtual assistants. While these applications rely on **large language models (LLMs) in the background**, they are categorized separately from **"LLM"** applications, which focus on **non-interactive** text processing tasks like document analysis and sentiment classification.

prevalent due to its robust capabilities for structured data processing, while GenAI and LLMs are increasingly adopted for tasks involving unstructured text or conversational interfaces.

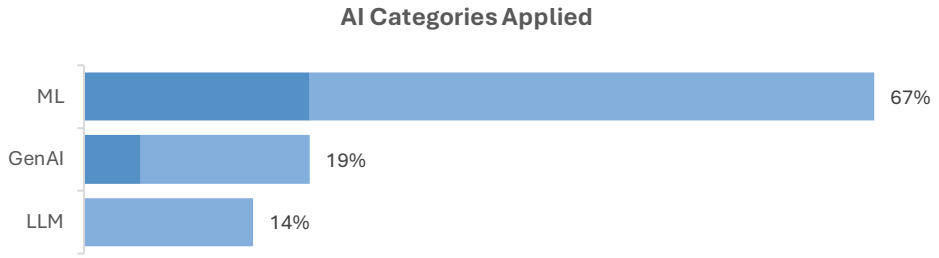


Figure 3: Distribution of AI categories applied in use cases (dark blue: Compliance use cases)

This distribution underscores the evolving adoption patterns of AI technologies in finance, with ML leading as a foundational tool and applications being used for many years already, and generative models like GenAI and LLMs gaining traction for more advanced or specialized applications.

3.3 Findings related to "Achieved or Intended Benefits"

The analysis of the 21 AI use cases reported by SFTI members reveals a diverse range of achieved or intended benefits. These benefits reflect the strategic priorities of financial institutions in leveraging AI technologies to enhance operational efficiency, reduce costs, and improve decision-making processes. The distribution of these benefits is summarized in the graph below (see Figure 4; multiple categories were applied), and the findings can be summarized as follows:

1. **Operational Efficiency (86%)**:
   The most frequently reported benefit, operational efficiency, is cited in 86% of the use cases. AI applications are streamlining processes, automating repetitive tasks, and reducing manual intervention. For example, fraud detection systems and customer onboarding solutions significantly enhance process speed and accuracy, allowing institutions to allocate resources more effectively.
2. **Cost Reduction (71%)**:
   Cost reduction ranks as the second most common benefit, reported in 71% of the use cases. AI-driven automation minimizes labor-intensive processes and operational costs while improving scalability. Applications such as AI-based chatbots and document processing tools exemplify how financial institutions achieve cost savings by replacing or augmenting traditional workflows.
3. **Risk Management and Compliance (33%)**:
   One-third of the use cases emphasize improved risk management and compliance as a key benefit. AI systems are being deployed to detect fraudulent activities, monitor trading patterns for market manipulation, and ensure adherence to regulatory requirements. These capabilities help institutions mitigate risks while maintaining trust and compliance with legal frameworks.
4. **Customer Experience and Satisfaction (33%)**:
   Enhancing customer experience is another priority, cited in 33% of the use cases. AI applications such as chatbots, sentiment analysis tools, and personalized marketing models enable institutions to provide tailored services and faster responses to customer needs, thereby improving satisfaction levels.
5. **Decision-Making Accuracy (29%)**:
   Nearly one-third of the use cases report improvements in decision-making accuracy as a benefit. By leveraging machine learning models and advanced analytics, financial institutions can

make data-driven decisions with greater precision, particularly in areas like fraud detection, credit scoring, and investment strategies.

6. **Data Insights and Analytics (29%)**:
   Another 29% of use cases highlight enhanced data insights as a key outcome. AI applications enable organizations to extract actionable insights from vast datasets, providing a deeper understanding of customer behavior, market trends, and operational performance.
7. **Scalability and Adaptability (19%)**:
   Scalability is cited as an intended benefit in 19% of the use cases. AI technologies allow financial institutions to handle increasing volumes of transactions or data without proportional increases in resources or costs, enabling them to adapt quickly to changing market demands.
8. **Revenue Generation and Upselling (5%)**:
   A smaller proportion (5%) of use cases focus on revenue generation through upselling opportunities or new product offerings enabled by AI tools such as recommendation engines or predictive analytics models.

The distribution of benefits reflects a clear prioritization of operational efficiency and cost reduction across financial institutions. These two benefits dominate because they directly address core business objectives such as reducing overheads and improving productivity. Secondary benefits like risk management, customer satisfaction, decision-making accuracy, and data insights demonstrate how AI is also being used strategically to enhance service quality and mitigate risks.

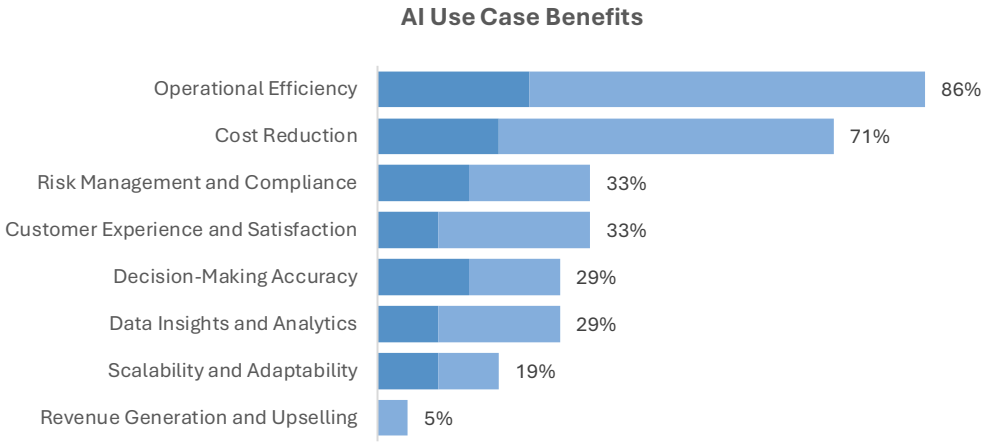


Figure 4: Distribution of Achieved or Intended Benefits of AI Use Cases (dark blue: Compliance use cases)

The reported benefits underscore the transformative potential of AI in finance. While operational efficiency and cost reduction remain primary drivers for adoption, secondary benefits like improved compliance, customer satisfaction, and decision-making accuracy highlight the broader strategic value that AI brings to financial institutions. This distribution also suggests that as organizations mature in their AI adoption journey, they may increasingly focus on advanced benefits like revenue generation and scalability to maintain competitive advantages in dynamic markets.

3.4 Findings related to "Use Case Life-Cycle"

The analysis of the 21 AI use cases reported by SFTI members provides insights into the life cycle stages of AI implementations in financial institutions. These stages reflect the maturity of AI projects, ranging from ideation to full deployment and scaling. The distribution of use cases across these stages is summarized in the graph below (see Figure 5; percentages have been rounded for clarity, and as a result, the total may slightly exceed 100%.), the findings related to the key life cycle stages indicated are as follows:

1. **Pilot Testing (43%)**:
   The largest proportion of use cases (43%) are in the pilot testing phase. At this stage, organizations validate the feasibility, performance, and impact of AI solutions on a smaller scale before committing to full deployment. Pilot testing allows institutions to identify potential issues, refine models, and ensure alignment with business objectives while minimizing risks.
2. **Full Deployment and Integration (29%)**:
   Nearly one-third of the use cases have progressed to full deployment and integration within operational systems. This stage involves embedding AI solutions into existing workflows, ensuring seamless interaction with legacy systems, and meeting compliance and security standards. Successful integration often requires collaboration across multiple departments, such as IT, risk management, and business units.
3. **Scaling and Optimization (19%)**:
   A smaller proportion of use cases (19%) have reached the scaling and optimization phase. This stage focuses on expanding the AI solution's scope across different business areas or geographies while improving its efficiency and accuracy through iterative refinements. Scalability is critical for maximizing the return on investment (ROI) of AI applications.
4. **Ideation and Feasibility Analysis (5%)**:
   Only 5% of use cases are in the initial ideation and feasibility analysis stage. This phase involves identifying potential AI opportunities, assessing their alignment with organizational goals, and determining technical feasibility.
5. **Development and Prototyping (5%)**:
   Another 5% of use cases are in the development and prototyping phase, where initial models or prototypes are built to test core functionalities before moving to pilot testing.
6. **Maintenance and Monitoring (0%)**:
   None of the reported use cases have yet reached the maintenance and monitoring phase. This stage typically involves ensuring continuous performance, addressing issues, retraining models with new data, and adapting to evolving business needs.
7. **End-of-Life or Decommissioning (0%)**:
   Similarly, no use cases have entered the end-of-life or decommissioning phase, which involves retiring outdated or underperforming AI systems.

The distribution highlights that most organizations are still in exploratory or early implementation stages, with a strong focus on pilot testing. This reflects a cautious approach to adopting AI technologies in finance, prioritizing validation before large-scale investments. The relatively small proportion of use cases in scaling or optimization stages suggests that AI adoption is still maturing within many institutions.

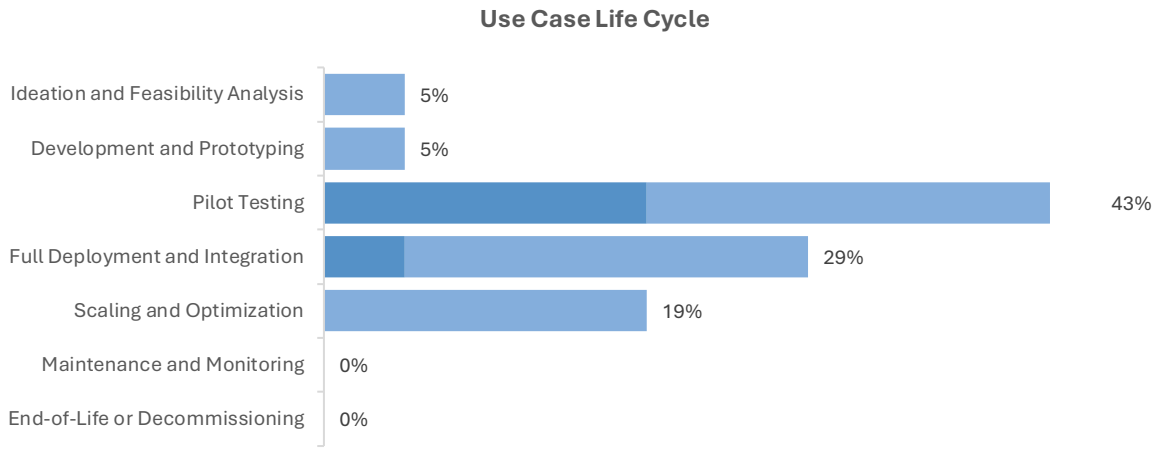


Figure 5: Distribution of AI Use Case Life Cycles (dark blue: Compliance use cases)

The life cycle distribution underscores a measured approach to AI adoption in financial institutions. While pilot testing dominates as organizations validate their solutions, there is significant progress toward full deployment and scaling for broader impact. As institutions gain experience with AI technologies, future trends may show increased activity in maintenance and optimization phases as solutions mature and deliver sustained value over time.

3.5 Decision Making Approaches for AI Use Cases

In the context of this study, "decision making approaches" relate to the internal process of " identifying and approving AI applications". The decision-making approaches reported by SFTI members highlight varying levels of maturity, governance, and stakeholder involvement. These approaches reflect how financial institutions balance innovation with compliance and risk management. The distribution of decision-making models, as shown in the graph below (see Figure 6), provides further insights into the prevalence of AI-specific frameworks. The key insights related to the decision-making approaches are as follows:

1. **AI-Specific Decision Models (37.5%)**:
   A minority of institutions (37.5%) reported using AI-specific decision-making models. These frameworks are tailored to address the unique challenges of AI, such as compliance with ethical and regulatory standards, data security concerns, and the need for transparency in algorithmic outputs. Institutions adopting AI-specific models often emphasize structured innovation processes, proof-of-concept (PoC) validation, and cross-functional collaboration.
2. **General Decision Models (62.5%)**:
   The majority of institutions (62.5%) do not use AI-specific decision-making frameworks. Instead, they treat AI projects similarly to other IT or business initiatives. While this approach simplifies integration into existing governance structures, it may lack the rigor required to address the complexities of AI technologies.

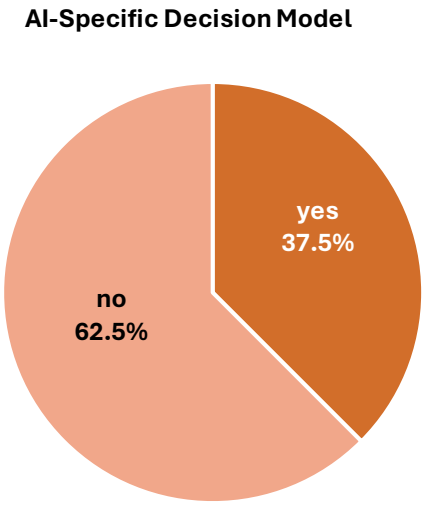


Figure 6: AI-Specific Decision Model

The reported decision-making approaches reveal a spectrum of practices ranging from general frameworks to highly structured AI-specific models. As a general principle, institutions leveraging tailored approaches are better positioned to address the unique challenges of AI adoption while ensuring compliance and maximizing value. As financial institutions continue their journey toward digital transformation, adopting best-in-class decision-making frameworks will be critical for achieving sustainable success with AI technologies.

The following common themes related to the decision-making approaches related to AI implementations have been shared through the survey:

- **Structured and Strategic Processes**:
  Companies 1 and 4 adopt structured frameworks that focus on innovation screening and PoC validation to assess the feasibility, desirability, and strategic alignment of AI applications. These processes help prioritize high-value use cases while minimizing risks.
- **Governance and Compliance**:
  Companies 4, 7, and 8 emphasize robust governance processes to ensure compliance with internal policies and external regulations (e.g., EU AI Act). This includes additional due diligence steps for AI applications to address security and risk concerns.
- **Decentralized vs. Centralized Decision-Making**:
  Company 6 employs a decentralized approach where individual departments lead decision-making under the oversight of a Chief Data Officer. In contrast, Companies 7 and 8 involve centralized governance bodies alongside cross-functional teams to ensure consistency.
- **Use-Case or Business-Case Driven Approaches**:
  Companies 1 and 8 evaluate AI applications based on their potential business impact, ensuring alignment with organizational objectives.
- **Lack of Defined Processes**:
  Some institutions (e.g., Companies 2, 3, and 5) lack formalized decision-making processes for AI applications, treating them as general technology projects without unique considerations.

Based on the responses given and insights shared, the following strategies for decision making related to the application of AI seem to be especially successful (see Table 1):

	Best-Practice Strategies for Decision-Making	
1.	**Innovation Screening**	▪ Identify high-value opportunities through structured processes or use-case evaluations.
2.	**Proof-of-Concept Validation**	▪ Conduct PoCs or pilots to assess feasibility, ROI potential, strategic fit, and compliance.
3.	**Governance Frameworks**	▪ Implement robust governance structures to ensure adherence to legal requirements (e.g., data protection laws) and ethical standards.
4.	**Cross-Functional Stakeholder Involvement**	▪ Engage diverse teams such as IT/cloud experts, legal/compliance departments, risk managers, procurement teams, SMEs, and business leaders.
5.	**Central Oversight with Decentralized Execution**	▪ Allow departments to lead implementation while maintaining centralized oversight for consistency.
6.	**Iterative Refinement**	▪ Use iterative processes to refine AI applications based on feedback from pilots or early implementations.

Table 1: Best-Practice Strategies for Decision-Making

3.6 AI-Specific Implementation Approaches

The analysis of the implementation approaches in the 21 AI use cases reveals that only a small proportion of financial institutions have adopted AI-specific implementation models. The distribution, as shown in the graph below (see Figure 7), highlights a significant reliance on general IT or project management frameworks.

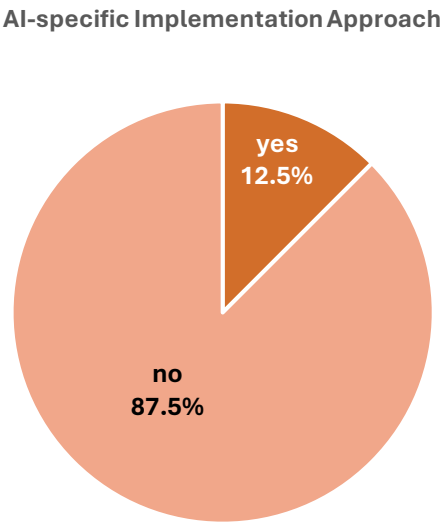


Figure 7: AI-Specific Implementation Approach

3.6.1 Key Insights related to AI-specific Implementation Approaches

1. **AI-Specific Implementation Approaches (12.5%)**:
   Only 12.5% of institutions reported using a dedicated AI-specific implementation approach. These organizations recognize the unique challenges posed by AI projects, such as compliance

with ethical and regulatory standards, data security concerns, and the need for iterative refinement. AI-specific approaches often include tailored governance frameworks, proof-of-concept (PoC) validation, and cross-functional collaboration to ensure successful deployment.

2. **General Implementation Approaches (87.5%)**:
   The majority of institutions (87.5%) treat AI projects similarly to other IT or business initiatives, relying on existing implementation models. While this approach simplifies integration into established processes, it may lack the rigor required to address the complexities of AI technologies, such as transparency in algorithmic decision-making or scalability challenges.

The dominance of general implementation approaches suggests that **many financial institutions are still in the early stages of their AI adoption journey**. The lack of tailored frameworks could hinder their ability to fully address the risks and opportunities associated with AI. However, institutions with AI-specific models are better positioned to manage these complexities and maximize value from their AI investments.

As such, the low adoption rate of AI-specific implementation approaches highlights an opportunity for financial institutions to enhance their readiness for complex AI projects. By integrating tailored methodologies into their implementation processes, organizations can better navigate the challenges of AI adoption while achieving greater operational efficiency and compliance. As the financial industry matures in its use of AI technologies, a shift toward more specialized frameworks is likely to emerge.

Based on the responses given and insights shared, the following strategies for implementing AI use cases seem to be especially successful (see Table 2):

	Best-Practice Strategies for AI-Specific Implementation Approaches
1. Tailored Governance Frameworks	▪ Establish governance structures that address data protection, ethical considerations, and regulatory compliance specific to AI applications.
2. Iterative Development Models	▪ Use PoCs and pilots to validate feasibility and refine solutions before full-scale deployment.
3. Cross-Functional Collaboration	▪ Involve diverse stakeholders such as IT teams, compliance officers, risk managers, and subject matter experts throughout the implementation process.
4. Scalability and Monitoring	▪ Design solutions with scalability in mind and implement continuous monitoring mechanisms to ensure sustained performance.

Table 2: Best-Practice Strategies for AI-Specific Implementation Approaches

3.6.2 Deep Dive: Implementation Approaches for AI Use Cases

The implementation approaches reported by SFTI members for AI applications in financial institutions reveal varying levels of standardization, governance, and agility. These approaches reflect the diverse ways organizations address the complexities of AI adoption while ensuring compliance, scalability, and alignment with strategic goals. The distribution of implementation approaches, as shown in the graph below (see Figure 8; percentages have been rounded for clarity, and as a result, the total may slightly exceed 100%), provides insights into the prevalence of specific methodologies.

3.6.3 Key Insights related to Specific Implementation Approaches for AI Use Cases

1. **Proof-of-Concept (PoC) and Iterative Models (38%)**:
   A significant proportion of institutions (38%) rely on PoC and iterative models to validate the feasibility of AI use cases. This approach helps identify technical and business gaps early in the process, allowing for iterative refinements before full deployment. For example, Company 1 emphasizes starting with PoCs to ensure alignment with business objectives.
2. **Standardized Frameworks (25%)**:
   About 25% of institutions adopt standardized frameworks such as the Scaled Agile Framework (SAFe). These frameworks provide a structured approach applicable to both AI and non-AI projects, ensuring consistency across implementations. Companies 4 and 5 exemplify this approach with their universal and phased models, such as "Discovery -> Definition -> Development -> Deployment -> Distribution."
3. **Compliance-Focused Models (19%)**:
   Compliance-focused approaches account for 19% of implementations. These models include additional steps for security, quality assurance, and adherence to regulatory standards. For instance, Company 7 employs dedicated tracking processes and forums to ensure transparency and compliance throughout the AI life cycle.
4. **General IT Project Models (13%)**:
   Institutions treating AI applications similarly to general IT projects represent 13% of the use cases. These organizations often lack specialized AI frameworks but aim to integrate AI into existing governance structures. Companies 2 and 8 illustrate this approach while building internal AI capabilities with external support.
5. **Data Governance-Centric Models (6%)**:
   A smaller proportion (6%) of institutions prioritize data governance as a core focus during implementation. For example, Company 3 plans to address data governance comprehensively as part of its broader AI strategy starting in 2025.

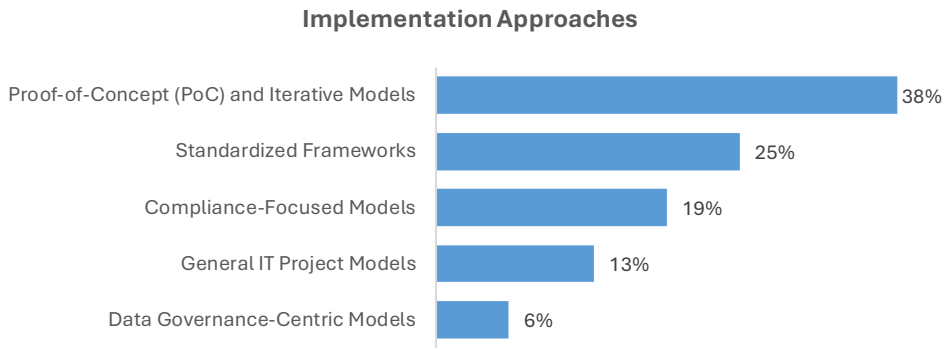


Figure 8:Distribution of Implementation Approaches

3.6.4 Common Themes in Implementation Approaches

- **Discovery and PoC Phase**:
  Institutions emphasize identifying high-value use cases through PoCs or pilots to validate feasibility and identify potential gaps.
- **Governance and Oversight**:
  Governance frameworks like the Three Lines of Defense (3LoD) are commonly applied to ensure compliance, risk management, and transparency.

- **Agile Practices**:
  Agile methodologies such as SAFe are adopted for flexibility and adaptability during implementation.
- **Compliance Integration**:
  Security, quality assurance, and adherence to regulatory standards are integral to many implementation models.

The distribution highlights that PoC-based iterative models dominate implementation approaches (38%), reflecting a cautious yet flexible strategy to validate AI solutions before scaling them. Standardized frameworks (25%) also play a significant role, offering consistency across projects. Compliance-focused models (19%) underscore the importance of adhering to regulatory requirements in financial institutions.

The reported implementation approaches highlight a mix of PoC-driven experimentation, standardized frameworks, compliance integration, and agile practices tailored to financial institutions' needs. As organizations mature in their AI adoption journey, combining these elements into a cohesive framework will be critical for ensuring scalability, compliance, and sustained value delivery from AI applications.

3.7 Key Success Factors for AI Use Cases

The analysis of the 21 AI use cases reported by SFTI members highlights several key success factors that contribute to the effective implementation of AI applications in financial institutions. These factors reflect the strategic, technical, and organizational considerations required to maximize the value of AI initiatives. The distribution of these success factors, as shown in the graph (see Figure 9; multiple categories were applied), and provides insights into their relative importance, and highlights specific key success factors, as follows:

1. **Strategic Alignment and Business Value (67%)**:
   Strategic alignment is one of the most frequently cited success factors, with 67% of use cases emphasizing its importance. Institutions prioritize aligning AI projects with business objectives and ensuring that measurable value—such as cost savings or revenue generation—is delivered. Proof-of-concept (PoC) validation is often used to confirm feasibility and expected outcomes.
2. **Internal Capabilities and Know-How (67%)**:
   Building internal expertise is equally critical, with 67% of use cases highlighting the need for skilled teams to design, develop, and manage AI solutions. Institutions stress reducing reliance on external providers by investing in training programs and fostering a culture of continuous learning.
3. **Governance, Compliance, and Ethical Standards (50%)**:
   Half of the use cases emphasize the importance of robust governance frameworks to ensure compliance with regulatory requirements (e.g., data protection laws) and ethical standards. Transparency and explainability in AI systems are also highlighted as essential for building trust among stakeholders.
4. **Data Quality and Availability (33%)**:
   High-quality data is identified as a foundational element for successful AI applications in 33% of use cases. Ensuring data availability, accuracy, and reusability is crucial for training reliable models and generating actionable insights.
5. **Stakeholder Engagement and Collaboration (33%)**:
   Early involvement of cross-functional teams—including compliance officers, legal experts, IT specialists, and business leaders—is cited in 33% of use cases. This collaboration ensures that AI projects address diverse organizational needs while fostering buy-in from key stakeholders.

6. **Change Management (33%)**:
   Managing organizational change is another critical factor mentioned in 33% of use cases. Institutions highlight the need for tailored training programs and proactive communication strategies to drive user adoption and overcome resistance to new technologies.
7. **Technology Readiness (17%)**:
   Technology readiness is identified as a success factor in 17% of use cases. This includes selecting appropriate tools, ensuring cloud infrastructure readiness, and designing scalable architectures to support advanced AI applications.
8. **Monitoring and Risk Awareness (17%)**:
   Continuous monitoring of AI systems is emphasized by 17% of use cases as a means to manage risks effectively. This includes tracking performance metrics, identifying potential biases, and retraining models as needed to maintain reliability over time.

The distribution illustrates that strategic alignment with business objectives and internal capabilities are the most frequently cited success factors, each appearing in 67% of use cases. Governance frameworks also play a significant role, reflecting the importance of compliance in highly regulated financial environments. Meanwhile, factors like technology readiness and monitoring are less commonly mentioned but remain critical for long-term success.

Figure 9: Distribution of Key Success Factors for AI Use Cases

Based on the responses given and insights shared, the following key success factors related to the application of AI seem to be most successful (see Table 3):

	Best-Practice Key Success Factors	
1.	**Strategic Alignment**	▪ Ensure that all AI initiatives align with overarching business goals and deliver measurable value through PoCs or pilots.
2.	**Invest in Internal Capabilities**	▪ Develop internal expertise through targeted training programs while fostering collaboration across departments.
3.	**Implement Robust Governance Frameworks**	▪ Establish clear guidelines for data protection, regulatory compliance, and ethical considerations to build trust among stakeholders.

4. Focus on Data Quality	▪ Invest in data management practices to ensure high-quality inputs for AI models.
5. Engage Stakeholders Early	▪ Involve cross-functional teams from the outset to address organizational needs comprehensively.
6. Proactive Change Management	▪ Develop tailored training programs and communication strategies to ensure user adoption.
7. Ensure Technology Readiness	▪ Select scalable tools and infrastructure capable of supporting future AI advancements.
8. Monitor Continuously	▪ Implement ongoing monitoring mechanisms to track performance metrics, address risks, and improve models iteratively.

Table 3: Best-Practice Key Success Factors

The reported key success factors underscore the multifaceted nature of implementing AI solutions in financial institutions. By focusing on strategic alignment, internal capabilities, governance frameworks, and stakeholder engagement, organizations can maximize the value derived from their AI initiatives while mitigating risks associated with adoption challenges. As financial institutions continue to mature in their use of AI technologies, these best practices will serve as a foundation for sustainable innovation and growth.

3.8 Key Challenges for AI Use Cases

The analysis of the 21 AI use cases reported by SFTI members reveals several key challenges encountered during the implementation of AI applications in financial institutions. These challenges span technical, organizational, and regulatory domains, reflecting the complexity of adopting AI technologies in a highly regulated and data-sensitive industry. The distribution of these challenges is summarized in the graph below (see Figure 10; multiple categories were applied), and highlights specific key challenges experienced during the AI implementation, as follows:

1. **Knowledge and Expertise (50%)**:
   Half of the use cases report a lack of internal expertise and domain knowledge as a major challenge. Institutions struggle with building AI engineering capabilities, understanding the value of AI, and addressing skills gaps in their workforce. This highlights the need for targeted hiring, training programs, and partnerships with external experts.
2. **Privacy, Security, and Data Usage (33%)**:
   Privacy and security concerns are cited in 33% of use cases, particularly when handling sensitive financial data in cloud environments. Challenges include obtaining client approval for data usage, ensuring data protection, and preventing potential leakage.
3. **Regulatory and Compliance Issues (33%)**:
   Regulatory uncertainty is another significant hurdle, particularly with evolving frameworks like the EU AI Act and FINMA Guidance 08/2024. Financial institutions face difficulties navigating compliance requirements for cloud-based AI services and ensuring adherence to ethical standards.
4. **Cultural and Organizational Challenges (33%)**:
   One-third of use cases highlight organizational readiness and cultural resistance as barriers to adoption. Institutions report delays caused by parallel projects (e.g., cloud foundation build-up) and a lack of data literacy among employees, which impedes effective adoption.
5. **Cost and ROI (17%)**:
   High costs and difficulty in calculating return on investment (ROI) are challenges in 17% of use cases. Institutions find it difficult to quantify initial investments and estimate the time required to develop and fine-tune AI models.

6. **System Integration (17%)**:
   Integrating AI applications into existing systems, such as CRM platforms or legacy IT infrastructures, is cited as a challenge by 17% of use cases due to complexity and high costs.
7. **Technical Limitations (17%)**:
   Limitations in current AI technologies are also reported in 17% of use cases. For example, large language models (LLMs) face constraints such as limited context size, weak reasoning capabilities, and insufficient domain expertise.

The distribution illustrates that **knowledge and expertise** is the most frequently cited challenge (50%), reflecting a widespread need for skill development within organizations. Privacy, regulatory compliance, and cultural challenges are also prominent, highlighting the importance of governance frameworks and change management strategies. Technical limitations, system integration issues, and cost concerns are less frequently mentioned but remain critical barriers to successful implementation.

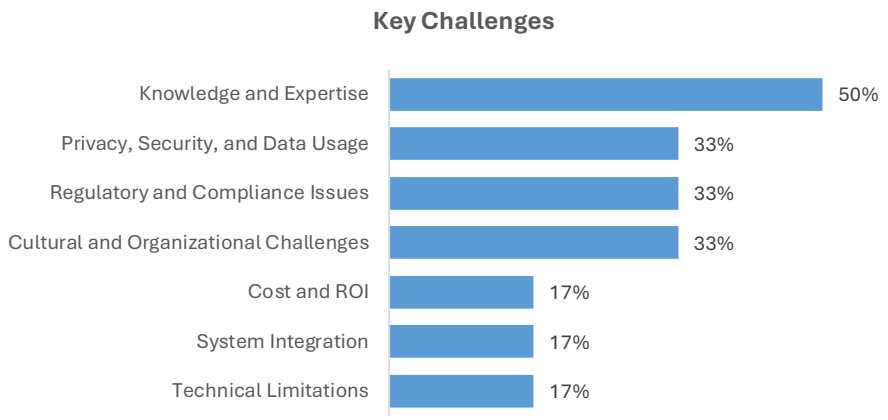


Figure 10: Distribution of Key Challenges during AI Use Case Implementation

Based on the responses given and insights shared, the following strategies for overcoming challenges experiences during the implementation of AI use cases seem to be most successful (see Table 4):

	Best-Practice Strategies for Overcoming Challenges
1. Building Knowledge and Expertise	▪ Targeted Hiring: Recruit professionals with expertise in AI engineering, data science, regulatory compliance, and organizational transformation. ▪ Training Programs: Implement ongoing education initiatives to upskill employees in technical areas like machine learning as well as soft skills like data literacy. ▪ External Partnerships: Collaborate with academic institutions or technology providers to bridge internal knowledge gaps.
2. Enhancing Privacy, Security, and Data Governance	▪ Develop robust data governance frameworks to ensure compliance with privacy regulations. ▪ Invest in secure cloud solutions with advanced encryption techniques to protect sensitive financial data. ▪ Establish clear policies for obtaining client consent for data usage.
3. Navigating Regulatory Complexity	▪ Proactively engage with regulators to understand evolving requirements like the EU AI Act and FINMA Guidance 08/2024. ▪ Implement compliance-by-design principles during AI development to ensure adherence to legal standards. ▪ Conduct regular audits to identify gaps in regulatory alignment.
4. Addressing Cultural Resistance	▪ Foster a culture of innovation by involving employees early in AI projects. ▪ Provide tailored training programs to improve data literacy across departments. ▪ Communicate the benefits of AI adoption clearly to build trust among stakeholders.
5. Managing Costs and Demonstrating ROI	▪ Use proof-of-concept (PoC) projects to validate feasibility before scaling. ▪ Conduct cost-benefit analyses early in the project lifecycle. ▪ Focus on high-impact use cases that deliver measurable business value.
6. Simplifying System Integration	▪ Adopt modular architectures that allow gradual integration into legacy systems without disrupting operations. ▪ Leverage APIs or middleware solutions to ensure seamless connectivity between new AI applications and existing platforms.
7. Overcoming Technical Limitations	▪ Invest in research to improve model capabilities or explore hybrid approaches combining human expertise with AI tools. ▪ Use task-specific models tailored to organizational needs rather than general-purpose solutions. ▪ Regularly retrain models with updated datasets to enhance performance over time.

Table 4: Best-Practice Strategies for Overcoming Challenges

The reported challenges underscore the complexity of implementing AI solutions in financial institutions. While knowledge gaps remain the most significant barrier, privacy concerns, regulatory

uncertainty, cultural resistance, cost issues, system integration challenges, and technical limitations also pose significant hurdles. By adopting best practices such as targeted training programs, robust governance frameworks, PoC validation processes, and scalable architectures, financial institutions can overcome these challenges effectively while maximizing the value derived from their AI initiatives. As organizations continue their journey toward digital transformation, addressing these barriers will be critical for achieving long-term success with AI technologies.

3.9 Other Notable Observations

The analysis of the 21 AI use cases provided by SFTI members reveals **several noteworthy trends and patterns that provide deeper insights** into the application of AI in financial institutions. These observations highlight variations in benefits, life-cycle stages, and implementation progress across different AI categories and use case domains.

Still, an important disclaimer must be made in this context: The study did not request respondents to provide quantitative data on the benefits of AI use cases. As such, a direct mathematical comparison between the benefits of different AI categories is not possible. However, for the purposes of this report, it is assumed that the mention of a greater number of benefit categories indicates that certain AI use cases may have the potential to deliver more diverse benefits compared to those reporting fewer benefit categories. As such, this interpretation is highly **indicative** and should be understood as such.

1. Benefits Across AI Categories

- **LLMs Report the Most Benefits**:
  Use cases applying **Large Language Models (LLMs)** report an average of **3.33 benefits per use case**, the highest among all AI categories. This reflects the versatility of LLMs in addressing text-heavy tasks such as sentiment analysis, document processing, and conversational agents.
- **ML Use Cases Are Close Behind**:
  Use cases applying **Machine Learning (ML)** report an average of **3.14 benefits per use case**, showcasing ML's effectiveness in structured data tasks like fraud detection, customer segmentation, and anomaly detection.
- **GenAI Reports Fewer Benefits**:
  Use cases involving **GenAI** report only **2.5 benefits per use case** on average. This may be due to its narrower focus on conversational interfaces and transcription tasks, which have more limited direct business impacts compared to ML or LLM applications.

2. Compliance vs. Non-Compliance Use Cases

- **Compliance Use Cases Yield More Benefits**:
  Use cases from compliance-related areas (e.g., fraud detection, trade surveillance) report an average of 3.2 benefits per use case, slightly higher than the 3 benefits per use case reported for non-compliance areas. This may indicate that AI applications in compliance functions are more mature and deliver broader organizational value.

3. Life-Cycle Maturity Across AI Categories

- **ML Use Cases Are More Advanced**:
  Machine Learning (ML) use cases show greater maturity, with some examples reaching the scaling and optimization phase. This reflects ML's long-standing adoption in financial services and its proven reliability for structured data tasks.
- **GenAI Use Cases Are in Early Deployment**:
  For GenAI, most use cases are either in full deployment (2 examples) or pilot testing (1 example). This indicates that generative AI applications are gaining traction but are still relatively new compared to ML.

- **LLM Use Cases Are Least Advanced**:
  Large Language Model (LLM) use cases remain in earlier stages, with most examples limited to pilot testing or development and prototyping phases. This highlights the emerging nature of LLM applications in financial institutions, where their potential is still being explored.

4. Observations on Implementation Approaches

- **Limited Adoption of AI-Specific Implementation Models**:
  Only 12.5% of use cases reported using an AI-specific implementation approach, while 87.5% relied on general IT project frameworks. This suggests that many institutions are still adapting their processes to address the unique challenges posed by AI technologies.

5. Strategic Alignment Drives Success

- Use cases with **clear alignment to strategic business objectives** tend to report more benefits and progress further along the life cycle. For example:
  Fraud detection and compliance-related use cases often align closely with risk management goals. **Customer-facing solutions** like chatbots focus on improving customer experience and operational efficiency.

The analysis reveals that while **Machine Learning remains the most mature and widely applied category**, Large Language Models show significant promise for delivering high-value benefits despite being at earlier life-cycle stages. Compliance-related use cases demonstrate higher average benefits, reflecting their critical role in addressing regulatory requirements. However, the limited adoption of AI-specific implementation models highlights a **need for financial institutions to tailor their processes to better support the unique demands of AI projects**. As institutions continue their journey toward AI maturity, focusing on strategic alignment, robust governance frameworks, and iterative development approaches will be critical for unlocking the full potential of these technologies across all domains.

4. Framework for Implementing AI in Swiss Financial Institutions

This framework provides a **structured approach to implementing AI in Swiss financial institutions**, integrating insights from the analysis of 21 AI use cases, key challenges, success factors, and best practices. The framework is designed to address the unique regulatory, organizational, and technological contexts of the Swiss financial industry.

4.1 Framework Overview

The implementation of Artificial Intelligence (AI) in Swiss financial institutions requires a structured framework that addresses the unique challenges and opportunities presented by AI technologies. This framework is designed to **guide institutions through every stage of their AI journey**, from identifying high-value use cases to scaling solutions while ensuring compliance with regulatory standards and alignment with business objectives.

The framework integrates insights from the analysis of 21 AI use cases, key success factors, challenges, and best practices identified in the Swiss financial industry. It also incorporates findings from various studies, guidelines and whitepapers on Artificial Intelligence (AI), Generative AI (GenAI), and other types of AI, which all emphasize the importance of explainability, governance, and incremental adoption strategies.

The framework is organized into six key elements: **Strategic Decision-Making**, **Governance and Compliance**, **Data Management**, **Implementation Approach**, **Organizational Readiness**, and **Monitoring and Risk Management** (see Figure 11).

Figure 11: Framework for Implementing AI in Swiss Financial Institutions

This visual structure emphasizes how each element contributes to a seamless and effective implementation process while addressing key challenges and leveraging success factors. The six Framework Elements are:

1. **Strategic Decision-Making**:
   Aligns AI projects with business goals, ensuring measurable value through innovation screening and PoC validation.
2. **Governance and Compliance**:
   Establishes robust frameworks to ensure adherence to legal, ethical, and regulatory standards (e.g., EU AI Act, FADP, FINMA Guidance 08/2024).
3. **Data Management**:
   Focuses on high-quality data governance, synthetic data generation for privacy, and advanced techniques like Retrieval-Augmented Generation (RAG).
4. **Implementation Approach**:
   Employs phased methodologies supported by agile practices for iterative development, deployment, and scaling.
5. **Organizational Readiness**:
   Addresses cultural resistance through change management while fostering innovation through training and leadership engagement.
6. **Monitoring and Risk Management**:
   Ensures continuous oversight of AI systems to detect biases, manage risks, and maintain performance over time.

This framework offers Swiss financial institutions a detailed roadmap to effectively navigate the complexities of AI implementation, ensuring both maximized business value and adherence to regulatory requirements. It is structured into logical components – the "what" – each accompanied by 105 clear, step-by-step instructions – the "how" – outlining the necessary actions, pertinent questions, and desired outcomes. While certain steps may appear repetitive across different elements and components of the framework, this repetition underscores their significance. Some steps might be optional in one context but mandatory in another, highlighting their critical role in the overall implementation process.

4.2 Element 1: Strategic Decision-Making

Strategic decision-making is the cornerstone of successfully implementing AI in Swiss financial institutions. It ensures that AI initiatives align with organizational objectives, deliver measurable business value, and address key challenges such as regulatory compliance and resource allocation. This section outlines the critical elements of strategic decision-making, emphasizing their relevance and practical steps for implementation.

The following table provides details on the individual components of this framework element and a step-by-step guide on how to best implement these (see Table 5).

Components of Framework Element 1: Strategic Decision-Making	
1.1 Innovation Screening	
Innovation screening helps identify high-value AI use cases that align with business priorities. By filtering potential applications based on feasibility, impact, and alignment with organizational goals, institutions can focus resources on projects with the greatest potential for success.	1. Identify **organizational pain points** or opportunities where AI can add value (e.g., fraud detection, customer interaction analysis). 2. Evaluate the feasibility of AI solutions using structured frameworks like **Retrieval-Augmented Generation (RAG)** for unstructured data or traditional ML models for structured data tasks. 3. **Prioritize use cases** based on expected ROI, compliance requirements, and alignment with strategic objectives.
1.2 Proof-of-Concept (PoC) Validation	
PoC validation ensures that proposed AI solutions are technically feasible and deliver the expected outcomes before scaling. This step minimizes risks associated with high costs or poor performance during full deployment.	4. **Define clear success metrics** for PoCs (e.g., accuracy, efficiency improvements). 5. **Test AI models on small-scale datasets** to validate their performance under real-world conditions. 6. Iterate on findings to **refine models and address gaps** before scaling.
1.3 Alignment with Business Objectives	
Aligning AI initiatives with business objectives ensures that projects contribute to organizational goals such as cost reduction, operational efficiency, customer satisfaction, or compliance adherence.	7. **Map each AI use case to specific business outcomes** (e.g., reducing customer churn or improving regulatory reporting). 8. **Engage stakeholders from relevant departments** (e.g., compliance, legal, IT, risk management and business units) to ensure alignment across functions. 9. **Regularly review progress** against predefined KPIs to ensure continued alignment.
1.4 Stakeholder Engagement	
Involving cross-functional teams early in the decision-making process ensures buy-in from key stakeholders and aligns technical capabilities with business needs.	10. **Identify stakeholders** from relevant departments such as compliance, legal, IT, risk management, and business units.

	11. **Conduct workshops** to gather input on priorities, risks, and desired outcomes for AI projects. 12. **Establish a governance committee** to oversee decision-making and ensure accountability throughout the AI lifecycle, incl. central oversight with clear roles, regular audits, and alignment with updated regulatory requirements for AI-specific risks.
1.5 Regulatory and Ethical Considerations	
Swiss financial institutions operate in a highly regulated environment where adherence to laws such as the Federal Data Protection Act (FADP) is critical. Addressing regulatory and ethical considerations early in the decision-making process mitigates risks of non-compliance.	13. **Assess regulatory requirements** for each use case (e.g., GDPR for data privacy). 14. **Incorporate explainability and transparency measures** into model design (e.g., audit trails for decision-making processes). 15. **Engage with regulators proactively** to clarify expectations for emerging technologies like Generative AI (GenAI).
1.6 Incremental Adoption	
Adopting AI incrementally allows organizations to learn from early implementations while minimizing risks associated with large-scale rollouts.	16. **Start with simple use cases** such as text summarization or chatbots before progressing to more complex applications like autonomous decision-making systems. 17. **Use a composable approach** where each stage builds on prior successes (e.g., transitioning from "Chat-to-Agent" to "Chat-to-Execution" systems).

Table 5: Components of Framework Element 1: Strategic Decision-Making

By following these steps, Swiss financial institutions can ensure that their AI initiatives are strategically aligned, technically feasible, and compliant with regulatory standards while delivering measurable business value.

4.3 Element 2: Governance and Compliance

Governance and compliance are critical elements of the framework for implementing AI in Swiss financial institutions. These elements ensure that AI systems adhere to legal, ethical, and regulatory requirements while addressing risks associated with data privacy, security, and transparency. Given the highly regulated nature of the financial industry in Switzerland, robust governance frameworks are essential to mitigate risks and build trust among stakeholders.

The following table provides details on the individual components of this framework element and a step-by-step guide on how to best implement these (see Table 6).

Components of Framework Element 2: Governance and Compliance	
2.1 Regulatory Adherence	
Swiss financial institutions must comply with local and international regulations, such as the Federal Data Protection Act (FADP), FINMA Guidance 08/2024, and the evolving EU AI Act. These regulations emphasize data privacy, explainability, and accountability in AI applications.	18. **Understand Regulatory Requirements**: Identify applicable laws and standards for each use case (e.g., GDPR for cross-border data usage). 19. **Compliance-by-Design**: Incorporate regulatory requirements into the design phase of AI systems to ensure adherence from the outset. 20. **Engage Regulators Proactively**: Collaborate with regulators to clarify expectations for emerging technologies like Generative AI (GenAI).
2.2 Ethical Standards	
Ethical considerations ensure that AI systems operate transparently, fairly, and without bias. This is particularly important in financial services, where decisions can significantly impact customers' lives.	21. **Establish Ethical Guidelines**: Define principles for fairness, transparency, and accountability in AI decision-making processes. 22. **Bias Mitigation**: Use techniques like reweighting data samples or adversarial training to reduce bias in AI models, integrate fairness evaluations into the lifecycle of AI systems and ensure compliance through third-party validations where necessary 23. **Human Oversight**: Integrate human-in-the-loop (HITL) systems to review critical outputs and ensure ethical compliance.
2.3 Explainability and Transparency	
Explainability is essential for building trust in AI systems, particularly in compliance-related use cases where decisions must be justified to regulators or clients	24. **Model Documentation**: Maintain centrally managed inventory of all AI systems incl. detailed records of model assumptions, testing, fallback mechanisms, training data, model architecture, and decision pathways. 25. **Source Attribution**: Clearly indicate the origin of generated content or decisions

	made by AI systems, incl. documentation of underlying logic, data sources, and reasoning pathways. 26. **Audit Trails**: Retain logs of user prompts and model outputs for post-hoc analysis and accountability.
2.4 Data Privacy and Security	
Handling sensitive financial data requires robust security measures to prevent breaches or misuse while ensuring compliance with privacy laws like Federal Data Protection Act (FADP).	27. **Data Governance Frameworks**: Implement policies for secure data storage, processing, and access control. 28. **Synthetic Data Generation**: Use synthetic data to train models without exposing sensitive information. 29. **Retrieval-Augmented Generation (RAG)**: Where relevant, enhance model outputs by retrieving verified external data sources while maintaining privacy.
2.5 Risk Management	
AI systems introduce unique risks such as model drift, hallucinations (plausible but incorrect outputs), and cybersecurity threats that must be proactively managed.	30. **Continuous Monitoring**: Track performance metrics like accuracy and error rates to detect deviations early. 31. **Feedback Filtering Mechanisms**: Evaluate user feedback quality before incorporating it into model updates. 32. **Cybersecurity Measures**: Implement advanced security protocols, including threat detection for AI-specific attacks (e.g., adversarial inputs or data poisoning). Regularly audit security measures to align with increased focus on operational risk mitigation for AI.

Table 6: Components of Framework Element 2: Governance and Compliance

By integrating these governance and compliance practices into their AI frameworks, Swiss financial institutions can navigate regulatory complexities effectively while building trust among stakeholders.

4.4 Element 3: Data Management

Data management is a foundational element in the successful implementation of AI in Swiss financial institutions. High-quality data is essential for training reliable AI models, ensuring compliance with regulatory requirements, and generating actionable insights. Given the sensitive and regulated nature of financial data, robust data governance frameworks are critical to address challenges related to privacy, security, and accuracy. This section provides a detailed narrative on the key components of data management, emphasizing their relevance and practical implementation.

The following table provides details on the individual components of this framework element and a step-by-step guide on how to best implement these (see Table 7).

Components of Framework Element 3: Data Management	
3.1 Data Quality and Availability	
The quality and availability of data directly impact the performance and reliability of AI models. Inaccurate, incomplete, or biased datasets can lead to flawed outputs, compromising decision-making processes and regulatory compliance.	33. **Data Cleaning and Preprocessing**: Ensure datasets are free from noise, redundancies, and inconsistencies to improve model accuracy. 34. **Data Augmentation**: Use techniques like reweighting or resampling to address imbalances in training datasets. 35. **Synthetic Data Generation**: Leverage synthetic data to create diverse and representative datasets while maintaining privacy.
3.2 Retrieval-Augmented Generation (RAG)	
RAG enhances the generative capabilities of AI models by retrieving relevant information from external data sources in real time. This approach improves response accuracy while maintaining compliance with privacy standards.	36. **Integrate RAG pipelines** into AI systems to retrieve verified data during inference. 37. **Use semantic search** mechanisms with vector databases for efficient information retrieval. 38. **Employ knowledge graph**-based RAG strategies for complex relationships between data points.
3.3 Privacy and Security	
Handling sensitive financial data requires robust measures to protect against breaches while ensuring compliance with privacy laws like the Federal Data Protection Act (FADP).	39. Implement **secure storage and access controls** for sensitive data. 40. **Use encryption techniques** for data in transit and at rest. 41. **Retain user prompts and outputs** for audit purposes while adhering to confidentiality requirements.
3.4 Data Governance Frameworks	
Strong governance frameworks ensure that data is managed responsibly throughout its lifecycle, from collection to processing and storage.	42. **Define roles and responsibilities** for data management across departments.

	43. **Establish policies** for data access, usage, and retention. 44. **Conduct regular audits** to ensure compliance with internal standards and external regulations, incl. enhanced due diligence for outsourced AI systems, vendor audits, and continuous monitoring of adherence to data governance standards.
3.5 Mitigating Hallucination Risks	
Hallucination refers to instances where AI models generate plausible but factually incorrect outputs due to poor-quality training data or inadequate architecture.	45. **Use RAG techniques** to cross-reference outputs with verified external sources. 46. **Incorporate human-in-the-loop (HITL) systems** for high-stakes decisions. 47. **Configure conservative model settings** to flag uncertainty rather than generate speculative responses
3.6 Tokenization Strategies	
Tokenization breaks down input text into smaller units (tokens) for model processing, affecting both performance and running costs.	48. **Select appropriate tokenization strategies** based on the complexity of tasks. 49. **Optimize token usage** to balance computational efficiency with response quality. 50. **Use dynamic content filters** during pre- and post-processing stages.

Table 7: Components of Framework Element 3: Data Management

By implementing these practices, Swiss financial institutions can ensure that their AI systems are built on a foundation of high-quality, secure, and well-governed data while mitigating risks associated with poor-quality inputs or hallucinated outputs.

4.5 Element 4: Implementation Approach

The implementation approach is a critical element in the successful adoption of AI technologies in Swiss financial institutions. It provides a structured pathway for integrating AI systems into existing processes while addressing risks, ensuring compliance, and maximizing business value. This section outlines the phased implementation approach, emphasizing its relevance, practical steps, and alignment with best practices.

The following table provides details on the individual components of this framework element and a step-by-step guide on how to best implement these (see Table 8).

Components of Framework Element 4: Implementation Approach	
4.1 Phased Implementation Model	
A phased approach allows institutions to minimize risks, validate feasibility, and iteratively improve AI solutions before full-scale deployment. This method is particularly effective in highly regulated environments like Swiss financial services, where compliance and risk mitigation are paramount.	**Discovery Phase** 51. Identify high-value use cases aligned with business goals (e.g., fraud detection, customer service automation). 52. Conduct initial feasibility studies to assess technical and operational requirements. **Definition Phase** 53. Define project scope, objectives, success metrics (e.g., ROI, accuracy), and resource needs. 54. Engage stakeholders from relevant departments (e.g., IT, compliance, legal, risk, business) to ensure alignment. **Development Phase** 55. Build AI models using agile methodologies like SAFe (Scaled Agile Framework). 56. Test models iteratively to ensure compliance with regulatory and ethical standards. **Deployment Phase** 57. Deploy solutions incrementally into production environments to minimize disruptions. 58. Monitor performance using predefined metrics to ensure reliability. **Distribution and Iteration Phase** 59. Scale solutions across the organization while incorporating user feedback for continuous improvement. 60. Retrain models with new data to maintain accuracy over time.

4.2 Agile Methodologies	
Agile methodologies provide flexibility during implementation, enabling teams to adapt quickly to changing requirements or unforeseen challenges.	61. **Use iterative cycles (sprints)** for development and testing phases. 62. **Incorporate frequent feedback loops** from stakeholders and end-users. 63. **Prioritize features** based on business impact and feasibility.
4.3 Integration with Legacy Systems	
Seamless integration of AI systems with existing IT infrastructure is essential for operational continuity and scalability.	64. **Use modular architectures** that allow gradual integration without disrupting core systems. 65. **Leverage APIs and middleware solutions** for connectivity between AI applications and legacy platforms. 66. **Conduct system compatibility tests** during the development phase.
4.4 Compliance Checks	
Compliance checks throughout the implementation process ensure adherence to legal and ethical standards, such as the Federal Data Protection Act (FADP) or EU AI Act and FINMA Guidance 08/2024.	67. **Conduct regular audits** of data usage, model outputs, and decision pathways. 68. **Implement explainability measures** like audit trails and source attribution for transparency. 69. **Engage compliance officers early** in the project lifecycle to address potential issues proactively.
4.5 Iterative Testing	
Iterative testing ensures that AI models meet performance benchmarks while addressing potential risks like bias or inaccuracies	70. **Use synthetic data or retrieval-augmented generation (RAG) techniques** for testing without exposing sensitive information. 71. **Evaluate models against predefined KPIs** such as accuracy, precision, recall, or F1 scores. 72. **Incorporate human-in-the-loop (HITL) systems** for validating high-stakes outputs.

Table 8: Components of Framework Element 4: Implementation Approach

By adopting this structured implementation approach, Swiss financial institutions can minimize risks while maximizing the value derived from their AI initiatives.

4.6 Element 5: Organizational Readiness

Organizational readiness is a critical element for successfully implementing AI in Swiss financial institutions. It addresses the cultural, structural, and skill-related factors that determine an institution's ability to adopt and scale AI technologies effectively. AI implementation requires not only technical capabilities but also a supportive organizational culture, strong leadership, and a workforce equipped with the necessary skills to embrace and manage AI-driven transformation.

The following table provides details on the individual components of this framework element and a step-by-step guide on how to best implement these (see Table 9).

Components of Framework Element 5: Organizational Readiness	
5.1 Change Management	
AI adoption often disrupts traditional workflows, requiring employees to adapt to new processes and tools. Effective change management ensures that the organization transitions smoothly while minimizing resistance and fostering acceptance	73. **Proactive Communication**: Clearly communicate the purpose, benefits, and expected outcomes of AI adoption to all stakeholders. 74. **Stakeholder Engagement**: Involve employees early in the process to address concerns and gather input on how AI can improve their work. 75. **Tailored Training Programs**: Provide targeted training to equip employees at all levels with the skills needed to decide on, use and manage AI tools effectively.
5.2 Upskilling and Reskilling	
AI adoption requires specialized skills in data science, machine learning, and AI governance. Upskilling existing employees and reskilling those in roles impacted by automation are critical for long-term success.	76. **Skill Gap Analysis**: Identify gaps in technical and soft skills required for AI implementation and operation. 77. **Training Programs**: Offer courses on data literacy, AI engineering, and ethical considerations for AI systems. 78. **Collaboration with External Partners**: Partner with academic institutions or technology providers to provide advanced training opportunities where necessary.
5.3 Leadership Buy-In	
Strong leadership is essential for driving organizational commitment to AI adoption. Leaders play a key role in setting strategic priorities, allocating resources, and fostering a culture of innovation.	79. **Define a Clear Vision**: Articulate how AI aligns with the institution's broader goals and values. 80. **Allocate Resources Strategically**: Ensure sufficient investment in technology infrastructure, training programs, and governance frameworks. 81. **Lead by Example**: Demonstrate enthusiasm for AI adoption by actively participating in pilot projects or training initiatives.

5.4 Fostering a Culture of Innovation	
A culture that embraces innovation is critical for sustaining momentum in AI adoption. Employees must feel empowered to experiment with new tools and processes without fear of failure.	82. **Encourage Experimentation**: Create sandboxes or test environments where employees can explore AI applications safely. 83. **Reward Innovation**: Recognize teams or individuals who contribute innovative ideas or successfully implement AI solutions. 84. **Break Down Silos**: Promote cross-departmental collaboration to ensure diverse perspectives are considered during implementation.
5.5 Addressing Cultural Resistance	
Resistance to change is a common challenge when introducing new technologies like AI. Addressing employee concerns proactively helps build trust and acceptance.	85. **Open Dialogue Channels**: Create forums where employees can voice concerns or ask questions about AI implementation. 86. **Highlight Benefits Over Risks**: Emphasize how AI will enhance roles rather than replace them. 87. **Provide Reassurance on Job Security**: Communicate that the primary goal of adopting AI is to augment human capabilities rather than eliminate jobs.

Table 9: Components of Framework Element 5: Organizational Readiness

By focusing on organizational readiness, Swiss financial institutions can create an environment where employees are empowered to embrace AI technologies as tools for growth, innovation, and enhanced efficiency.

4.7 Element 6: Monitoring and Risk Management

Monitoring and risk management are essential components of the framework for implementing AI in Swiss financial institutions. These elements ensure that AI systems perform reliably, remain compliant with regulatory standards, and mitigate risks such as model drift, hallucinations, and cybersecurity threats. Given the high stakes in financial services, robust monitoring and risk management practices are critical to maintaining trust, minimizing errors, and ensuring long-term success.

The following table provides details on the individual components of this framework element and a step-by-step guide on how to best implement these (see Table 10).

Components of Framework Element 6: Monitoring and Risk Management	
6.1 Continuous Monitoring	
Continuous monitoring ensures that AI systems maintain their performance and accuracy over time. It helps detect deviations in outputs caused by changes in data patterns, system updates, or evolving regulatory requirements.	88. **Performance Metrics**: Track key metrics such as accuracy, precision, recall, F1 scores (which provide a balanced measure of precision and recall), and error rates to assess system performance continuously. 89. **Automated Alerts**: Implement alert systems to notify administrators when performance metrics fall below predefined thresholds, or in case of deviations in accuracy, model drift, and operational robustness. 90. **Regular Audits**: Conduct periodic audits of AI systems to evaluate compliance with internal policies and external regulations, including stress testing and bias detection protocols as required.
6.2 Bias Detection and Mitigation	
Bias in AI models can lead to unfair or discriminatory outcomes, particularly in applications like credit scoring or fraud detection. Detecting and mitigating bias is crucial to maintaining ethical standards and regulatory compliance.	91. **Bias Audits**: Regularly evaluate training datasets for imbalances or biases that could influence model outputs. 92. **Adversarial Training**: Use techniques like adversarial training or reweighting to reduce bias during model development. 93. **Human Oversight**: Incorporate human-in-the-loop (HITL) systems to review high-stakes decisions for potential bias.
6.3 Hallucination Risk Management	
Hallucination refers to instances where AI models generate plausible but factually incorrect outputs. This is a significant risk in applications requiring high accuracy, such as regulatory reporting or customer service automation.	94. **Retrieval-Augmented Generation (RAG)**: Implement RAG techniques to cross-reference outputs with verified external data sources for accuracy.

	95. **Conservative Model Settings**: Configure models to flag uncertainty rather than generate speculative responses when confidence is low. 96. **Human Validation:** Use HITL systems to validate outputs in high-stakes scenarios.
6.4 Cybersecurity Measures	
AI systems are vulnerable to cybersecurity threats such as prompt injection attacks, data poisoning, or adversarial manipulations that can compromise their reliability and security.	97. **Robust Security Protocols**: Implement encryption for data at rest and in transit, along with secure access controls. 98. **Attack Detection Systems**: Deploy mechanisms to detect and mitigate AI application-specific attacks like prompt injection or adversarial inputs. 99. **Content Filters**: Use pre- and post-processing filters to ensure that outputs align with ethical standards and business requirements.
6.5 Feedback Loop Management	
Feedback loops can degrade model performance if user inputs inadvertently reinforce undesirable behaviors or biases.	100. **Feedback Filtering Mechanisms**: Evaluate the quality of user feedback before incorporating it into model updates. 101. **Controlled Retraining Cycles**: Avoid continuous learning from user feedback by implementing controlled retraining cycles with validated data. 102. **Diverse Feedback Sources**: Incorporate feedback from a broad range of users to avoid overfitting or degradation caused by limited input diversity.
6.6 Model Drift Prevention	
Model drift occurs when an AI system's performance degrades over time due to changes in real-world data patterns that differ from the training dataset.	103. **Regular Retraining**: Update models periodically with new datasets to align them with current trends and conditions. 104. **Drift Detection Metrics**: Monitor metrics like prediction accuracy and consistency of outputs to identify signs of drift early. 105. **Automated Alerts for Drift Detection**: Notify administrators when drift is detected so corrective actions can be taken promptly.

Table 10: Components of Framework Element 6: Monitoring and Risk Management

By integrating these monitoring and risk management practices into their AI frameworks, Swiss financial institutions can ensure that their AI systems remain reliable, secure, and aligned with business objectives while mitigating potential risks effectively.

5. Scalability of the Framework for Implementing AI in Swiss Financial Institutions

Scalability is a critical consideration for implementing AI in financial institutions, as it determines the ability to expand AI systems across different use cases, departments, or geographies without requiring significant changes to the underlying framework. The proposed framework for implementing AI in Swiss financial institutions is inherently scalable, ensuring that its elements can support growth and adaptation as needs evolve. This chapter explores the scalability of the framework, emphasizing that no fundamental changes are required to cater to scaling needs. It also provides insights into scaling AI within financial institutions in general.

5.1 Scalability of the Framework

The framework for implementing AI in Swiss financial institutions has been meticulously designed with flexibility and modularity at its core, ensuring it **can scale effectively to meet evolving needs**. Each component of the framework is crafted to support incremental growth, allowing institutions to adapt and expand without undergoing fundamental structural changes.

At its foundation, **strategic decision-making** ensures that innovation remains at the forefront. The framework incorporates processes like innovation screening, which can be adapted to evaluate new and emerging use cases. Proof-of-concept (PoC) validation plays a crucial role in this stage, emphasizing scalability from the outset by focusing on high-impact applications that have the potential for broader implementation across the organization.

The **governance and compliance** element is equally robust, prepared to address increasing complexity as AI systems expand across departments or regions. By adhering to compliance-by-design principles, the framework ensures that regulatory requirements are seamlessly integrated into systems, maintaining consistent adherence regardless of scale.

Data management is another pillar of the framework, providing a solid foundation for scalability through robust data governance strategies. These frameworks ensure data quality and accessibility, even as datasets grow larger and sources become more diverse. Techniques such as Retrieval-Augmented Generation (RAG) and synthetic data generation are employed to maintain efficiency and safeguard data privacy and security, enabling institutions to scale their AI systems confidently.

The **implementation approach** is designed to be phased and methodical, following a progression from discovery to distribution. This phased model enables institutions to build incrementally on the success of pilot projects. Modular architectures and agile methodologies further enhance this component, allowing for the seamless integration of new systems and use cases as they emerge.

Preparing the organization for AI adoption is another crucial aspect of the framework. Scalable training programs ensure that employees at all levels are equipped with the knowledge and skills needed as AI becomes more prevalent. At the same time, change management strategies address potential resistance, fostering a culture that embraces innovation and continuous learning.

Finally, **monitoring and risk management** are integral to the framework's scalability. Continuous monitoring systems are designed to handle increasingly complex models and larger datasets, while proactive risk management practices mitigate the possibility of vulnerabilities or performance issues arising during scaling.

In essence, this framework offers a cohesive and forward-looking approach, enabling Swiss financial institutions to navigate the complexities of AI adoption with confidence and precision. By aligning strategic planning, compliance, data governance, implementation, organizational readiness, and risk management, it creates a pathway for sustainable growth and innovation in the digital age (see Table 11).

	Framework Element	Scalability Considerations
1.	**Strategic Decision-Making**	▪ The innovation screening process can be expanded to evaluate additional use cases as new opportunities emerge. ▪ Proof-of-concept (PoC) validation ensures that scalability is built into projects from the start by identifying high-impact use cases with potential for broader application.
2.	**Governance and Compliance**	▪ Governance frameworks are designed to handle increasing complexity as AI systems scale across departments or regions. ▪ Compliance-by-design principles ensure that regulatory adherence remains consistent regardless of system size or scope.
3.	**Data Management**	▪ Robust data governance frameworks support scalability by ensuring data quality and availability across larger datasets and diverse sources. ▪ Techniques like Retrieval-Augmented Generation (RAG) and synthetic data generation enable efficient scaling without compromising data privacy or security.
4.	**Implementation Approach**	▪ The phased implementation model (Discovery → Definition → Development → Deployment → Distribution) allows for incremental scaling by building on successful pilots. ▪ Modular architectures and agile methodologies facilitate seamless integration of new use cases or systems.
5.	**Organizational Readiness**	▪ Training programs can be scaled to include more employees as AI adoption grows within the institution. ▪ Change management strategies ensure that cultural resistance is addressed at every stage of scaling.
6.	**Monitoring & Risk Management**	▪ Continuous monitoring systems can accommodate larger datasets and more complex models as AI systems expand. ▪ Proactive risk management practices ensure that scaling does not introduce new vulnerabilities or performance issues.

Table 11: Scalability Considerations per Framework Element

5.2 Scaling AI Within Financial Institutions

Scaling AI within financial institutions requires a deliberate and structured approach, enabling a smooth transition from small-scale pilots to organization-wide applications while preserving high standards of performance, regulatory compliance, and operational efficiency. Achieving this expansion involves several critical considerations, each designed to ensure scalability without compromising quality.

The journey begins with **incremental scaling**, focusing initially on straightforward use cases such as automating routine workflows. These simpler applications lay the groundwork for more complex implementations like fraud detection or regulatory reporting. By adopting a composable approach, institutions can build on the successes of earlier stages, allowing their risk management and control frameworks to mature alongside the expanding scope of AI applications.

Infrastructure readiness forms another cornerstone of successful scaling. As AI systems grow, they require robust IT infrastructure capable of handling larger datasets, greater model complexity, and increasing user demands. Cloud-based solutions and hybrid architectures provide the flexibility and scalability necessary to accommodate this growth, ensuring that technological limitations do not impede progress.

Scaling AI also demands effective **cross-functional collaboration**. Involving departments such as IT, compliance, and legal ensures alignment with organizational objectives and regulatory standards. Open communication between these teams fosters a collaborative environment, enabling challenges to be addressed collectively and with greater agility.

To **maintain performance** across a broader application of AI systems, institutions must prioritize continuous model optimization. Regular retraining with updated datasets ensures accuracy in evolving contexts. Techniques such as Parameter-Efficient Fine-Tuning (PEFT) and Low-Rank Adaptation (LoRA) offer ways to optimize performance without incurring excessive computational costs, preserving efficiency while enhancing capability.

Risk mitigation remains a critical focus as AI systems scale. Increased usage can introduce risks such as model drift, hallucination effects, or feedback loop degradation. Continuous monitoring systems are essential to detect and address these risks promptly. Additionally, robust cybersecurity measures are vital to safeguard systems against vulnerabilities that may emerge as the scale of operations grows.

Finally, **realizing business value** is central to the scaling process. By targeting high-impact use cases at each stage of implementation, institutions can deliver measurable benefits, including cost savings, enhanced operational efficiency, and improved customer satisfaction. Establishing clear metrics to quantify return on investment (ROI) ensures that AI initiatives remain aligned with broader business goals (see Table 12).

Institutional Expansion	*Scalability Considerations*
1. **Incremental Scaling**	▪ Start with simple use cases (e.g., automating routine workflows) before progressing to complex decision-making applications like fraud detection or regulatory reporting. ▪ Use a composable approach where each stage builds on prior successes, allowing risks and controls to mature progressively.
2. **Infrastructure Readiness**	▪ Ensure that IT infrastructure is capable of supporting increased data volumes, model complexity, and user demands. ▪ Adopt cloud-based solutions or hybrid architectures for flexibility and scalability.
3. **Cross-Functional Collaboration**	▪ Involve multiple departments (e.g., IT, compliance, legal) in scaling efforts to ensure alignment with organizational goals and regulatory requirements. ▪ Foster communication between teams to address challenges collaboratively.
4. **Performance Optimization**	▪ Regularly retrain models with updated datasets to maintain accuracy as they are applied to new contexts. ▪ Use techniques like Parameter-Efficient Fine-Tuning (PEFT) or Low-Rank Adaptation (LoRA) to optimize performance without excessive computational costs.
5. **Risk Mitigation**	▪ Monitor for model drift, hallucination risks, and feedback loop degradation as systems scale. ▪ Implement robust cybersecurity measures to protect against vulnerabilities that may arise with increased usage.
6. **Business Value Realization**	▪ Focus on high-impact use cases that deliver measurable business value at each stage of scaling. ▪ Quantify ROI through metrics such as cost savings, operational efficiency improvements, or enhanced customer satisfaction.

Table 12: Scalability Considerations for Institutional Expansion

The **modularity and flexibility** of the proposed framework ensure that it can accommodate scaling without requiring significant modifications:

- Each element of the framework is designed to operate **independently** while integrating seamlessly with other components.
- The **phased implementation approach** inherently supports incremental growth by building on prior successes.
- Governance frameworks and compliance **measures are robust** enough to handle increased complexity as systems scale.
- **Training programs and change management** strategies can be adapted to include more employees or address new challenges without altering their core structure.

This comprehensive approach to scaling AI enables financial institutions in Switzerland to maximize the potential of AI technologies across their operations. By leveraging best practices, including incremental scaling, modular architectures, and continuous monitoring, they can expand efficiently, maintain compliance, and deliver significant business value without introducing unnecessary risks.

6. Conclusions and Recommendations

This chapter synthesizes the key findings of the study and provides actionable recommendations for Swiss financial institutions seeking to implement AI effectively and sustainably. The conclusions are structured into four subchapters: decision-making and implementation recommendations, key success factors for implementation, key challenges and strategies to overcome them, and other general recommendations. Together, these sections offer a comprehensive roadmap for navigating the complexities of AI adoption while ensuring compliance, scalability, and alignment with organizational goals.

6.1 Decision-Making and Implementation Recommendations

The study underscores the importance of structured decision-making processes and phased implementation strategies in ensuring the success of AI initiatives. Institutions should begin by **identifying high-value use cases** through systematic **innovation screening**. This involves **engaging cross-functional teams** to assess organizational priorities and areas where AI can **deliver measurable value**. **Proof-of-concept (PoC) validation** is a critical step in this process, as it allows institutions to test feasibility, refine models, and demonstrate potential return on investment (ROI) before scaling solutions.

Implementation should follow a **phased approach**, beginning with discovery and definition phases to establish clear objectives, followed by development, deployment, and scaling phases. **Agile methodologies**, such as the Scaled Agile Framework (SAFe), provide flexibility during implementation, enabling institutions to adapt quickly to changing requirements or unforeseen challenges.

Governance frameworks play a central role in decision-making and implementation. Institutions must integrate **compliance-by-design principles** into their AI systems to **address regulatory requirements proactively**. Transparency measures, such as audit trails and explainability mechanisms, are essential for building trust among stakeholders.

A summary overview is provided below (see Table 13), for further details on decision-making approaches and implementation models, refer to Chapter 4.5 "Decision-Making Approaches for AI Use Cases" and Chapter 4.6 "AI-Specific Implementation Approaches."

	Decision Making and Implementation Recommendations	
1.	**Identify Use Cases**	▪ Conduct innovation screening to prioritize high-value applications aligned with business goals.
2.	**Validate Feasibility**	▪ Perform PoCs or pilots to assess technical viability, ROI potential, and compliance risks.
3.	**Develop Governance Frameworks**	▪ Establish clear guidelines for data protection, ethical considerations, and regulatory compliance.
4.	**Build Internal Capabilities**	▪ Invest in training programs and cross-functional collaboration.
5.	**Implement in Phases**	▪ Use agile methodologies for iterative development, deployment, scaling, and optimization.
6.	**Monitor Continuously**	▪ Track performance metrics, address risks proactively, and retrain models as needed.

Table 13: Summary of Decision Making and Implementation Recommendations

6.2 Key Success Factors for Implementation

An in-depth analysis of 21 AI use cases within financial institutions has identified several critical success factors essential for effective implementation. Foremost among these is **strategic alignment**, ensuring that AI initiatives are closely integrated with the organization's overarching goals. This alignment facilitates the delivery of measurable business value, enabling institutions to achieve cost reductions, enhance operational efficiencies, and elevate customer satisfaction.

Equally important is the development of robust **internal capabilities**. Sustaining AI initiatives over the long term necessitates building internal expertise. Investing in targeted training programs to upskill employees in areas such as data science, machine learning, and governance is crucial. This investment not only fosters a culture of continuous learning but also ensures that the institution possesses the necessary skills to manage and advance AI projects effectively.

Governance and compliance form another cornerstone of successful AI implementation. Establishing robust governance frameworks ensures adherence to regulatory requirements and addresses ethical considerations, including fairness and transparency. Institutions must prioritize compliance with Swiss regulations, such as the Federal Data Protection Act (FADP), FINMA Guidance 08/2024, and align with international frameworks like the EU AI Act. This commitment safeguards the institution's integrity and fosters trust among stakeholders.

The **quality of data** utilized in AI applications cannot be overstated. High-quality data serves as the foundation for successful AI outcomes. Institutions should implement comprehensive data governance frameworks that guarantee data availability, accuracy, and privacy. Such frameworks ensure that AI systems operate on reliable information, leading to more accurate and trustworthy results.

Managing organizational change is pivotal in fostering acceptance of AI technologies. Addressing cultural resistance through tailored training programs and proactive communication strategies helps employees understand the benefits of AI adoption. This approach cultivates a supportive environment where innovation can thrive.

Lastly, designing AI systems with **scalability in mind** from the outset enables institutions to expand their AI initiatives efficiently. By planning for growth, organizations can scale AI applications without necessitating significant structural changes, thereby maintaining continuity and minimizing disruptions.

A summary overview is provided below (see Table 14), for a more comprehensive exploration of these success factors, refer to Chapter 4.8, "Key Success Factors for AI Use Cases."

	Key Success Factors for Implementation
1. Strategic Alignment	▪ Aligning AI initiatives with organizational goals ensures that projects deliver measurable business value. Institutions that prioritize strategic alignment are better positioned to achieve cost reductions, operational efficiencies, and enhanced customer satisfaction.
2. Internal Capabilities	▪ Building internal expertise is essential for sustaining AI initiatives over the long term. Institutions should invest in targeted training programs to upskill employees in data science, machine learning, and governance.
3. Governance and Compliance	▪ Robust governance frameworks ensure adherence to regulatory requirements while addressing ethical considerations such as fairness and transparency. Institutions must prioritize compliance with Swiss regulations like the Federal Data Protection Act (FADP), FINMA Guidance 08/2024 and international frameworks such as the EU AI Act.

4. Data Quality	▪ High-quality data is a cornerstone of successful AI applications. Institutions should establish data governance frameworks that ensure data availability, accuracy, and privacy
5. Change Management	▪ Managing cultural resistance is critical for fostering acceptance of AI technologies within organizations. Tailored training programs and proactive communication strategies can help employees understand the benefits of AI adoption.
6. Scalability	▪ Designing scalable systems from the outset enables institutions to expand their AI initiatives efficiently without requiring structural changes

Table 14: Summary of Key Success Factors for Implementation

6.3 Key Challenges and How to Overcome Them

Implementing artificial intelligence (AI) within Swiss financial institutions presents a multifaceted array of challenges that must be navigated to harness its full potential. A significant hurdle is the prevalent **knowledge gap**, particularly in AI engineering and governance. Many institutions find themselves lacking the internal expertise necessary to develop and manage AI systems effectively. To bridge this gap, collaboration with academic partners and technology providers becomes essential, alongside substantial investment in employee training programs to cultivate the requisite skills. Implementing cross- and up-skilling initiatives can further enhance the workforce's adaptability, ensuring that employees are equipped to meet the evolving demands of AI integration.

Privacy concerns further complicate AI implementation, especially given the sensitive nature of financial data. Compliance with regulations such as the Federal Data Protection Act (FADP) is imperative. Employing techniques like synthetic data generation and retrieval-augmented generation (RAG) can mitigate privacy risks while preserving data utility, ensuring that data-driven AI models do not compromise client confidentiality.

The **regulatory landscape adds another layer of complexity**. Navigating evolving frameworks, including the newly published FINMA Guidance 08/2024 and the EU AI Act, poses challenges, particularly for institutions operating across multiple jurisdictions. Proactive engagement with regulators is crucial to clarify compliance expectations and to adapt swiftly to regulatory changes, thereby avoiding potential legal pitfalls.

Cultural resistance within organizations also poses a significant barrier. Employees may harbor concerns about job displacement or may not fully grasp the benefits of AI integration. Addressing these apprehensions through open dialogue and strong leadership support is vital to foster a culture of innovation and acceptance.

From a technical standpoint, **integrating AI systems into existing legacy infrastructures** can be resource-intensive and complex. Adopting modular architectures and application programming interfaces (APIs) can facilitate smoother integration, minimizing operational disruptions and ensuring that new AI systems work harmoniously with established processes.

Moreover, AI models are susceptible to issues such as **hallucination risks and model drift** over time, which can degrade their performance. Implementing regular retraining protocols with updated datasets, coupled with human-in-the-loop (HITL) systems, can effectively address these challenges, maintaining the accuracy and reliability of AI applications.

A summary overview is provided below (see Table 15), for an in-depth exploration of these challenges and strategies to overcome them, refer to Chapter 4.9, "Key Challenges for AI Use Cases."

Key Challenges and How to Overcome Them	
1. Knowledge Gaps	▪ The lack of internal expertise in AI engineering and governance is a significant barrier. Institutions can address this by collaborating with academic partners or technology providers to bridge skill gaps while investing in employee training programs, combined with institutional cross- and up-skilling initiatives.
2. Privacy Concerns	▪ Handling sensitive financial data requires robust privacy measures to comply with regulations like the FADP. Techniques such as synthetic data generation and Retrieval-Augmented Generation (RAG) can help mitigate privacy risks while maintaining data utility.
3. Regulatory Complexity	▪ Navigating evolving regulatory frameworks, such as the FINMA Guidance 08/2024 and the EU AI Act, poses challenges for institutions operating across borders. Proactive engagement with regulators can help clarify compliance expectations.
4. Cultural Resistance	▪ Employees may resist adopting new technologies due to concerns about job displacement or lack of understanding of AI's benefits. Institutions should foster a culture of innovation by addressing these concerns through open dialogue and leadership support.
5. System Integration	▪ Integrating AI systems into legacy infrastructures can be resource-intensive. Modular architectures and APIs can facilitate seamless integration while minimizing disruptions.
6. Technical Limitations	▪ Current AI models may face limitations such as hallucination risks or model drift over time. Regular retraining with updated datasets and human-in-the-loop (HITL) systems can address these issues effectively.

Table 15: Summary of Key Challenges and How to Overcome Them

6.4 Other General Recommendations

To maximize the benefits of AI adoption and effectively navigate associated challenges, Swiss financial institutions should adopt a **structured and deliberate approach** that balances innovation with risk management. One of the **most effective strategies is incremental scaling**. By starting with small, focused pilot projects, institutions can minimize risks, gain valuable insights from early implementations, and refine their strategies before expanding solutions across the organization.

Focusing on **high-impact use cases** is equally essential. By prioritizing applications that align closely with organizational objectives and deliver measurable outcomes, institutions can ensure that their AI investments yield tangible benefits, such as improved operational efficiency, cost savings, or enhanced customer satisfaction.

The **adoption of modular architectures** is another critical recommendation. These architectures enable the seamless integration of AI systems into existing infrastructures, reducing operational disruptions and providing the flexibility needed for gradual scaling. This approach not only preserves system stability but also facilitates the iterative addition of new functionalities.

Continuous monitoring plays a pivotal role in maintaining the reliability and effectiveness of AI systems over time. By implementing robust performance tracking mechanisms, institutions can

detect and address issues such as model drift or declining accuracy, ensuring that their AI applications remain fit for purpose.

Engaging stakeholders early in the AI adoption process is crucial for success. Collaboration across diverse teams—including IT, compliance, legal, risk management, and business units—ensures that AI initiatives are well-rounded and aligned with both operational and regulatory requirements. Early involvement fosters buy-in and facilitates smoother implementation.

Lastly, **preparing for cross-border compliance readiness** is essential in an increasingly globalized regulatory environment. Aligning internal policies with international standards, such as the EU AI Act, positions institutions to adapt proactively to regulatory changes, reducing compliance risks and enhancing operational resilience.

These recommendations form a comprehensive framework for Swiss financial institutions to navigate the complexities of AI adoption effectively. By emphasizing compliance, scalability, and alignment with organizational goals, institutions can unlock the transformative potential of AI technologies while managing associated risks (see Table 16).

	Other General Recommendations	
1.	**Adopt Incremental Scaling**	▪ Start small with pilot projects before expanding successful solutions organization-wide. This approach minimizes risks while allowing institutions to learn from early implementations.
2.	**Focus on High-Impact Use Cases**	▪ Prioritize applications that align closely with organizational goals and deliver measurable benefits.
3.	**Leverage Modular Architectures**	▪ Design systems that allow gradual integration into existing infrastructures without disrupting operations.
4.	**Monitor Continuously**	▪ Implement performance tracking mechanisms to ensure that AI systems remain reliable over time.
5.	**Engage Stakeholders Early**	▪ Involve diverse teams from IT, compliance, legal, risk management, and business units throughout the decision-making process.
6.	**Foster Cross-Border Compliance Readiness**	▪ Prepare for regulatory changes by aligning internal policies with international standards like the EU AI Act.

Table 16: Summary of Other General Recommendations

7. Appendix

7.1 AI Use Case Details

No	Compliance Use Case?	Use Case Description	Category of AI Used	Benefits								Life-Cycle						
				Operational Efficiency	Cost Reduction	Risk Management and Compliance	Customer Experience and Satisfaction	Decision-Making Accuracy	Data Insights and Analytics	Scalability and Adaptability	Revenue Generation and Upselling	Ideation and Feasibility Analysis	Development and Prototyping	Pilot Testing	Full Deployment and Integration	Scaling and Optimization	Maintenance and Monitoring	End-of-Life or Decommissioning
01	no	AI Assistant to transcribe customer calls	GenAI	x	x					x				x				
02	no	Fraud detection within payment transactions	ML			x										x		
03	no	Digital client onboarding, customer identification via Video and Passport	ML	x	x		x									x		
04	no	Voice Biometrics, customer identification via voice	ML	x	x	x	x									x		
05	no	Fraud detection (Classification Models)	ML	x	x	x		x							x			
06	yes	Second opinion system to filter out false positives flagged by AMLT rule engine	ML	x	x									x				
07	no	Alarming of suspicious activity in corporate accounts	ML	x					x						x			
08	no	Customer Interaction Analysis, systematic analysis of customer feedbacks	LLM				x		x					x				
09	no	Different Marketing AI-Models to segment customers	ML				x				x					x		
10	no	AI Assistant to transcribe and summarize customer calls	GenAI	x	x		x											
11	no	AI-driven chatbot-like assistant in MS Office apps	GenAI	x											x			
12	no	Various HR applications: candidate profile matching, automated application screening, etc.	ML	x	x			x				X						
13	yes	Closure of generated matches in Name Matching Customer application	ML	x	x	x									x			
14	no	Microsoft Co-Pilot	GenAI	x	x			x							x			
15	no	Product Scoring Application	ML	x	x	x		x	x					x	x			
16	yes	Fraud Detection	ML	x	x	x	x							x				
17	no	Document Analysis and Archivation	LLM	x	x				x	x				x				
18	no	Customer Online Identification	ML	x	x			x		x				x				
19	yes	Hedonic Real Estate Pricing Model	ML	x	x	x	x		x	x				x				
20	yes	Trade surveillance solution analyzing trading activity	ML	x				x	x					X				
21	no	Voice- and Chatbot (AI-Agent Framework, selection of LLMs, e.g., Bedrock models)	LLM	x	x		x		x	x			x					

Table 17: AI Use Case Details

7.2 List of Tables

7.3 List of Figures

7.4 References

Ankenbrand et. al. (2023) GPT for Financial Advice - The Combination of Large Language Models and Rule-Based Systems. Retrieved from https://hub.hslu.ch/retailbanking/wp-content/uploads/sites/7/2023/05/GPT-for-Financial-Advice-2023.pdf

BDO. (2024). The EU AI Act and its implications for Swiss companies. Retrieved from https://www.bdo.ch/en-gb/insights/the-eu-ai-act-and-its-implications-for-swiss-companies

Chahal, M. (2023). Automating financial regulatory compliance with AI. Finance & Accounting Research Journal, 6(4), 1035-1258.

Chambers and Partners. (2024). Artificial intelligence 2024: Trends and developments in Switzerland. Authors: Cornelia Stengel, Luca Stäuble. Retrieved from https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/switzerland/trends-and-developments

Deloitte Switzerland. (2024). EU Artificial Intelligence Act: Implications for Swiss Companies. Retrieved from https://www2.deloitte.com/ch/en/pages/financial-advisory/articles/eu-artificial-intelligence-act.html

Deloitte Switzerland. (2024). Legal landscape of AI regulations in the European Union and Switzerland. Retrieved from https://blogs.deloitte.ch/tax/2024/02/legal-landscape-of-ai-regulations-in-the-european-union-and-switzerland.html

EY. (2023). How artificial intelligence is reshaping the financial services industry. Retrieved from https://www.ey.com/en_gr/financial-services/how-artificial-intelligence-is-reshaping-the-financial-services-industry

FDPIC. (2023). Current Data Protection Legislation Applicable to AI. Retrieved from https://www.edoeb.admin.ch/edoeb/en/home/kurzmeldungen/2023/20231109_ki_dsg.html

FINMA. (2023). Artificial intelligence in the Swiss financial market (2023). Retrieved from https://www.finma.ch/en/documentation/dossier/dossier-fintech/kuenstliche-intelligenz-im-schweizer-finanzmarkt-2023/

FINMA. (2023). Artificial Intelligence: FINMA's Supervisory Expectations. Retrieved from https://www.finma.ch/en/documentation/dossier/dossier-fintech/kuenstliche-intelligenz/

FINMA. (2024). FINMA Guidance 08/2024: Governance and risk management when using artificial intelligence. Retrieved from: https://www.finma.ch/en/news/2024/12/20241218-mm-finma-am-08-24/

FSB. (2024). Financial Stability Board (FSB): The Financial Stability Implications of Artificial Intelligence. Retrieved from https://www.fsb.org/uploads/P14112024.pdf

Global Legal Insights. (2024). AI, Machine Learning & Big Data Laws 2024 | Switzerland. Retrieved from https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/switzerland

Grant Thornton. (2023). Dealing with Artificial Intelligence in a Regulated Environment. Retrieved from https://www.grantthornton.ch/en/insights/artifical-intelligence-in-regulated-environment/

Griesinger (2024). Schweizerisches Datenschutzgesetz: Datenschutz-Compliance für Unternehmen beim Einsatz von KI-Anwendungen. In: Der Compliance Berater, CB 2024/12. Retrieved from https://online.ruw.de/suche/cb/Schweizer-Datenschutz-Datens-Compli-fuer-Untern-be-3171d30e1a6f39e719806600d760197e

International Compliance Association (ICA). (2023). The rise of AI and its impact on compliance. Retrieved from https://www.int-comp.org/insight/the-rise-of-ai-and-its-impact-on-compliance/

Kodex AI & Deutsche Bank Whitepaper (2024). Adopting Generative AI in Banking. Retrieved from attached whitepaper document.

MAS. (2024). Monetary Authority of Singapore (MAS): Artificial Intelligence (AI) Model Risk Management – Observations from a Thematic Review. Retrieved from: https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/artificial-intelligence-model-risk-management

MME Legal | Tax | Compliance. (2023). FINMA's Supervisory Expectations Regarding the use of Artificial Intelligence of Supervised Entities. Retrieved from https://www.mme.ch/en/magazine/articles/finmas-supervisory-expectations-regarding-the-use-of-artificial-intelligence-of-supervised-entities

Modulos.ai. (2023). Switzerland's Approach to AI Regulation in the Financial Sector. Retrieved from https://www.modulos.ai/blog/switzerland-ai-regulation-financial-sector/

Mogaji, E., et al. (2022). The evolution of Artificial Intelligence in financial services: Implications for marketing strategies. Journal of Financial Services Marketing.

OECD (2024). Artificial Intelligence in Finance. Retrieved from https://www.oecd.org/en/topics/sub-issues/digital-finance/artificial-intelligence-in-finance.html

Patil, S. (2023). Transformative impact of Artificial Intelligence on financial services industry: A review of recent advancements. Journal of Business Research.

PwC Switzerland. (2024). The Artificial Intelligence Act demystified. Retrieved from https://www.pwc.ch/en/insights/regulation/ai-act-demystified.html

Ridzuan et.al. (2024). Ridzuan et. al.: AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility. Retrieved from https://www.mdpi.com/2078-2489/15/8/432

Roland Berger (2024). Mastering AI in the Finance Function. Retrieved from https://www.rolandberger.com/en/Insights/Publications/Mastering-AI-in-the-finance-function.html

SAFe. (2024). The Scaled Agile Framework (SAFe). Retrieved from: https://safe.scaledagile.com/en/unauthenticated

SAS Institute (2021). AI in Banking: Survey Reveals Factors for Success. Retrieved from https://www.sas.com/en_ae/insights/articles/analytics/ai-in-banking-survey-reveals-factors-for-success.html

Stengel, C. (2023). Die Schweiz braucht kein KI-Gesetz. Retrieved from https://www.fuw.ch/die-schweiz-braucht-kein-ki-gesetz-794705355805

SWI swissinfo.ch. (2024). Has Switzerland missed the train on AI regulation? Retrieved from https://www.swissinfo.ch/eng/business/has-switzerland-missed-the-train-of-ai-regulation/49055386

Swiss Federal Data Protection and Information Commissioner (FDPIC). (2023). Current data protection legislation is directly applicable to AI. Retrieved from https://www.edoeb.admin.ch/edoeb/en/home/kur-zmeldungen/2023/20231109_ki_dsg.html

Swiss Finance Council. (2024). SFC response to EC consultation on AI in financial services. Retrieved from https://www.swissfinancecouncil.org/news-views/positions/175-sfc-response-to-ec-consultation-on-ai-in-financial-services

SwissBanking. (2023). Data protection and data governance. Retrieved from https://www.swissbanking.ch/en/financial-centre/information-for-bank-clients-and-companies/data-protection-and-data-governance

White & Case LLP. (n.d.). AI Watch: Global regulatory tracker - Switzerland. Retrieved from https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-switzerland